Fedora 13

Manual de virtualización

La guía definitiva de virtualización en Fedora

Christopher Curran

Fedora 13 Manual de virtualización
La guía definitiva de virtualización en Fedora
Edición 0

Autor Christopher Curran ccurran@redhat.com

Copyright © 2008,2009,2010 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at *http://creativecommons.org/licenses/by-sa/3.0/*. The original authors of this document, and Red Hat, designate the Fedora Project as the "Attribution Party" for purposes of CC-BY-SA. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, MetaMatrix, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

For guidelines on the permitted uses of the Fedora trademarks, refer to *https://fedoraproject.org/wiki/Legal:Trademark_guidelines*.

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

Java® is a registered trademark of Oracle and/or its affiliates.

XFS® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

All other trademarks are the property of their respective owners.

La Guía de virtualización de Fedora contiene información acerca de la instalación, configuración, administración, y procedimientos para la solución de los problemas relacionados con tecnologías de virtualización utilizadas en Fedora.

Por favor tenga en cuenta que: Este documento aún se encuentra en desarrollo, y por tal motivo está sujeto a numerosas modificaciones, y se ofrece aquí con la característica de provisorio. El contenido y las instrucciones que se pueden encontrar aquí no deberían considerarse como finalizados, y deberían ser utilizados con precaución.

Prefacio **vii**
1. Acerca de este libro vii
2. Convenciones del Documento vii
2.1. Convenciones Tipográficas vii
2.2. Convenciones del documento ix
2.3. Notas y Advertencias ix
3. ¡Necesitamos sus comentarios! x

I. Requerimientos y limitaciones **1**

1. Requerimientos del sistema **3**

2. Compatibilidad de KVM **5**

3. Limitaciones de virtualización **7**
3.1. Limitaciones generales para virtualización 7
3.2. Limitaciones de KVM 7
3.3. Limitaciones de aplicación 8

II. Instalación **11**

4. Instalación de paquetes virtuales **13**
4.1. Instalación de KVM con instalación nueva de Fedora 13
4.2. Instalación de paquetes KVM en un sistema Fedora existente 15

5. Introducción a la instalación de un huésped virtualizado **17**
5.1. Consideraciones y pre requisitos relacionados con los huéspedes virtualizados..... 17
5.2. Creación de huéspedes con virt-install 18
5.3. Creación de huéspedes con virt-manager 18
5.4. Instalación de huéspedes con PXE 31

6. Cómo instalar Linux para empresas de Red Hat 5 como un huésped completamente virtualizado **37**

7. Instalación de Windows XP como huésped completamente virtualizado **47**

8. Instalación de Windows Server 2003 como un huésped completamente virtualizado **67**

9. Installing Windows Server 2008 como huésped totalmente virtualizado **71**

III. Configuración **83**

10. Dispositivos de almacenamiento virtualizados **85**
10.1. Cómo crear un controlador de disquete virtualizado 85
10.2. Cómo añadir dispositivos de almacenaje a huéspedes 86
10.3. Cómo configurar almacenamiento persistente en Fedora 90
10.4. Cómo añadir dispositivos CD-ROM o DVD a un huésped 92

11. Configuración de la red **93**
11.1. Traducción de dirección de red (NAT) con libvirt 93
11.2. Creación de redes en puente con libvirt 94

12. Controladores KVM para-virtualizados **97**
12.1. Instalacion de controladores KVM Windows para-virtualizados 97
12.2. Cómo instalar controladores con un disquete virtualizado 109

12.3. Uso de controladores KVM para-virtualizados para dispositivos existentes 109
12.4. Uso de controladores KVM para-virtualizados para nuevos dispositivos 110

13. Puente PCI 115
13.1. Cómo agregar un dispositivo PCI com virsh 116
13.2. Cómo agregar un dispositivo PCI con virt-manager 118
13.3. Puentes PCI con virt-install 123

14. SR-IOV 125
14.1. Introducción 125
14.2. Cómo útilizar SR-IOV 126
14.3. Cómo solucionar problemas relacionados con SR-IOV 129

15. Frase de acceso del dispositivo USB 131

16. Virtualización de ID de N_Port (NPIV, por las iniciales en inglpes de N_Port ID Virtualization) 133

17. Administración del tiempo del huésped KVM 135

IV. Administración 139

18. Mejores prácticas de servidor 141

19. Seguridad para la virtualización 143
19.1. Problemas en la seguridad del almacenamiento 143
19.2. SELinux y virtualización completas 143
19.3. SELinux 145
19.4. Información del cortafuegos de virtualización 146

20. Migración en vivo KVM 147
20.1. Requerimientos de migración en vivo 148
20.2. Ejemplo de almacenaje compartido: NFS para una migración sencilla 148
20.3. Migración KVM en vivo con virsh 149
20.4. Migración con virt-manager 150

21. Administración remota de huéspedes virtualizados 161
21.1. Administración remota con SSH 161
21.2. Administración remota en TLS y SSL 163
21.3. Modos de transporte 163

22. KSM 169

23. Advanced virtualization administration 171
23.1. Guest scheduling 171
23.2. Advanced memory management 171
23.3. Guest block I/O throttling 171
23.4. Guest network I/O throttling 171

24. Migración de Xen a KVM 173
24.1. Xen a KVM 173
24.2. Versiones viejas de KVM a KVM 173

25. Tareas de administración diversas 175
25.1. Cómo iniciar los huéspedes automáticamente 175
25.2. Cómo utilizar qemu-img 175
25.3. Sobrealojamiento con KVM 177
25.4. Cómo verificar las extensiones de virtualización 178

25.5. Cómo acceder a los datos desde una imagen de huésped de disco 180
25.6. Cómo configurar las afinidades de un procesador KVM 182
25.7. Cómo generar una nueva y única dirección MAC 186
25.8. `ftpd` muy seguro 187
25.9. Cómo configurar persistencia LUN 188
25.10. Deshabilitar monitoreo de discos SMART para los huéspedes 189
25.11. Cómo configurar un servidor VNC 189

V. Cuestiones relacionadas con el almacenamiento en virtualización **191**

26. Usando almacenamiento compartido con imágenes de disco virtuales **193**
26.1. Usando ISCSI para almacenar imágenes de discos virtuales. 193
26.2. Usando NFS para almacenar imágenes de discos virtuales 193
26.3. Usando GFS2 para almacenar discos virtuales. 193
26.4. Grupos de almacenamiento 193
26.4.1. Configurando dispositivos de almacenamiento para grupos 193
26.4.2. Direccionamiento virtualizado de los huéspedes a los grupos de almacenamiento 193

VI. Guía de referencia de virtualización **195**

27. Herramientas de virtualización **197**

28. Administración de huéspedes virtuales con virsh **199**

29. Manejo de huéspedes con un Administrador de máquinas virtuales (virt-manager) **209**
29.1. La ventana de agregado de conexión 209
29.2. La ventana principal del Administrador de máquinas virtuales 210
29.3. La pestaña de visión general del huésped 211
29.4. Consola gráfica de la Máquina virtual 212
29.5. Cómo iniciar virt-manager 213
29.6. Restaurar una máquina guardada 214
29.7. Mostrar información de huéspedes 216
29.8. Estado de monitorización 222
29.9. Mostrar los identificadores de huésped 224
29.10. Displaying a guest's status 225
29.11. Mostrar las CPU virtuales 226
29.12. Mostrar uso de la CPU 227
29.13. Mostrar uso de memoria 228
29.14. Administración de una red virtual 229
29.15. Crear una nueva red virtual 230

30. referencia de configuración de libvirt **239**

31. Creación de scripts libvirt personales **241**
31.1. Uso de los archivos de configuración XML con virsh 241

VII. Solución de problemas **243**

32. Solución de problemas **245**
32.1. Herramientas de depuración, y de solución de problemas 245
32.2. Archivos de registro 246
32.3. Solución de problemas con consolas seriales 247

32.4. Archivos de registro de virtualización 247
32.5. Errores del dispositivo en bucle 248
32.6. Habilitando las extensiones de virtualización de hardware Intel VT y AMD-V en BIOS 248
32.7. Desempeño del entorno de red de KVM 249

A. Recursos adicionales **251**
A.1. Recursos en línea 251
A.2. Documentación instalada 251

Glosario **253**

B. Historial de revisiones **259**

C. Colofón **261**

Prefacio

Este libro es la Guía de virtualización de Fedora. Cubre todos los aspectos relacionados con la utilización y la administración de los productos de virtualización ofrecidos en Fedora.

1. Acerca de este libro

Este libro se divide en 7 partes:

- Requerimientos del sistema
- Instalación
- Configuración
- Administración
- Referencia
- Trucos y consejos
- Solución de problemas

Los conceptos fundamentales y los términos utilizados en este documento, se encuentran explicados con más detalle en el glosario, *Glosario*.

Este documento describe cuestiones relacionadas con la virtualización en Fedora. El hipervisor *Máquinas virtuales basadas en el Kernel* es ofrecido con Fedora. El hipervisor KVM ofrece soporte para *Virtualización completa*.

2. Convenciones del Documento

Este manual utiliza varias convenciones para resaltar algunas palabras y frases y llamar la atención sobre ciertas partes específicas de información.

En ediciones PDF y de papel, este manual utiliza tipos de letra procedentes de *Liberation Fonts*[1]. Liberation Fonts también se utilizan en ediciones de HTML si están instalados en su sistema. Si no, se muestran tipografías alternativas pero equivalentes. Nota: Red Hat Enterprise Linux 5 y siguientes incluyen Liberation Fonts predeterminadas.

2.1. Convenciones Tipográficas

Se utilizan cuatro convenciones tipográficas para llamar la atención sobre palabras o frases específicas. Dichas convenciones y las circunstancias en que se aplican son las siguientes:

`Negrita monoespaciado`

Utilizada para resaltar la entrada del sistema, incluyendo comandos de shell, nombres de archivo y rutas. También se utiliza para resaltar teclas claves y combinaciones de teclas. Por ejemplo:

> Para ver el contenido del archivo **`my_next_bestselling_novel`** en su directorio actual de trabajo, escriba el comando **`cat my_next_bestselling_novel`** en el intérprete de comandos de shell y pulse **`Enter`** para ejecutar el comando.

[1] https://fedorahosted.org/liberation-fonts/

El ejemplo anterior incluye un nombre de archivo, un comando de shell y una tecla clave. Todo se presenta en negrita-monoespaciado y distinguible gracias al contexto.

Las combinaciones de teclas se pueden distinguir de las teclas claves mediante el guión que conecta cada parte de una combinación de tecla. Por ejemplo:

> Pulse **Enter** para ejecutar el comando.
>
> Pulse **Control**+**Alt**+**F1** para cambiar a la primera terminal virtual. Pulse **Control**+**Alt**+**F7** para volver a su sesión de Ventanas-X.

La primera oración resalta la tecla clave determinada que se debe pulsar. La segunda resalta dos conjuntos de tres teclas claves que deben ser presionadas simultáneamente.

Si se discute el código fuente, los nombres de las clase, los métodos, las funciones, los nombres de variables y valores de retorno mencionados dentro de un párrafo serán presentados en **Negrita-monoespaciado**. Por ejemplo:

> Las clases de archivo relacionadas incluyen **filename** para sistema de archivos, **file** para archivos y **dir** para directorios. Cada clase tiene su propio conjunto asociado de permisos.

Negrita proporcional

Esta denota palabras o frases encontradas en un sistema, incluyendo nombres de aplicación, texto de cuadro de diálogo, botones etiquetados, etiquetas de cajilla de verificación y botón de radio; títulos de menú y títulos del sub-menú. Por ejemplo:

> Seleccionar **Sistema** → **Preferencias** → **Ratón** desde la barra del menú principal para lanzar **Preferencias de Ratón**. En la pestaña de **Botones**, haga clic en la cajilla **ratón de mano izquierda** y luego haga clic en **Cerrar** para cambiar el botón principal del ratón de la izquierda a la derecha (adecuando el ratón para la mano izquierda).
>
> Para insertar un caracter especial en un archivo de **gedit**, seleccione desde la barra del menú principal **Aplicaciones** → **Accesorios** → **Mapa de caracteres**. Luego, desde la barra del menú **mapa de caracteres** elija **Búsqueda** → **Hallar…**, teclee el nombre del caracter en el campo **Búsqueda** y haga clic en **Siguiente**. El caracter buscado se resaltará en la **Tabla de caracteres**. Haga doble clic en este caracter resaltado para colocarlo en el campo de **Texto para copiar** y luego haga clic en el botón de **Copiar**. Ahora regrese a su documento y elija **Editar** → **Pegar** desde la barra de menú de **gedit**.

El texto anterior incluye nombres de aplicación; nombres y elementos del menú de todo el sistema; nombres de menú de aplicaciones específicas y botones y texto hallados dentro de una interfaz gráfica de usuario, todos presentados en negrita proporcional y distinguibles por contexto.

Itálicas-negrita monoespaciado o ***Itálicas-negrita proporcional***

Ya sea negrita monoespaciado o negrita proporcional, la adición de itálicas indica texto reemplazable o variable. Las itálicas denotan texto que usted no escribe literalmente o texto mostrado que cambia dependiendo de la circunstancia. Por ejemplo:

> Para conectar a una máquina remota utilizando ssh, teclee **ssh** ***nombredeusuario@dominio.nombre*** en un intérprete de comandos de shell. Si la

máquina remota es **example.com** y su nombre de usuario en esa máquina es john, teclee **ssh john@example.com**.

El comando **mount -o remount *file-system*** remonta el sistema de archivo llamado. Por ejemplo, para volver a montar el sistema de archivo **/home**, el comando es **mount -o remount /home**.

Para ver la versión de un paquete actualmente instalado, utilice el comando **rpm -q *paquete***. Éste entregará el resultado siguiente: ***paquete-versión-lanzamiento***.

Observe las palabras en itálicas- negrita sobre — nombre de usuario, domain.name, sistema de archivo, paquete, versión y lanzamiento. Cada palabra es un marcador de posición, tanto para el texto que usted escriba al ejecutar un comando como para el texto mostrado por el sistema.

Aparte del uso estándar para presentar el título de un trabajo, las itálicas denotan el primer uso de un término nuevo e importante. Por ejemplo:

Publican es un sistema de publicación de *DocBook*.

2.2. Convenciones del documento

Los mensajes de salida de la terminal o fragmentos de código fuente se distinguen visualmente del texto circundante.

Los mensajes de salida enviados a una terminal se muestran en **romano monoespaciado** y se presentan así:

```
books        Desktop   documentation  drafts  mss    photos   stuff  svn
books_tests  Desktop1  downloads      images  notes  scripts  svgs
```

Los listados de código fuente también se muestran en **romano monoespaciado**, pero se presentan y resaltan de la siguiente manera:

```
package org.jboss.book.jca.ex1;

import javax.naming.InitialContext;

public class ExClient
{
   public static void main(String args[])
       throws Exception
   {
      InitialContext iniCtx = new InitialContext();
      Object         ref    = iniCtx.lookup("EchoBean");
      EchoHome       home   = (EchoHome) ref;
      Echo           echo   = home.create();

      System.out.println("Created Echo");

      System.out.println("Echo.echo('Hello') = " + echo.echo("Hello"));
   }
}
```

2.3. Notas y Advertencias

Finalmente, utilizamos tres estilos visuales para llamar la atención sobre la información que de otro modo se podría pasar por alto.

Nota

Una nota es una sugerencia, atajo o enfoque alternativo para una tarea determinada. Ignorar una nota no debería tener consecuencias negativas, pero podría perderse de algunos trucos que pueden facilitarle las cosas.

Importante

Important boxes detail things that are easily missed: configuration changes that only apply to the current session, or services that need restarting before an update will apply. Ignoring a box labeled 'Important' won't cause data loss but may cause irritation and frustration.

Advertencia

Las advertencias no deben ignorarse. Ignorarlas muy probablemente ocasionará pérdida de datos.

3. ¡Necesitamos sus comentarios!

Si encuentra un error tipográfico en este manual o si sabe de alguna manera de mejorarlo, nos gustaría escuchar sus sugerencias. Por favor complete un reporte en Bugzilla: *http://bugzilla.redhat.com/bugzilla/* usando el producto **Fedora Documentation**.

When submitting a bug report, be sure to mention the manual's identifier: *virtualization-guide*

Si tiene una sugerencia para mejorar la documentación, intente ser tan específico como sea posible cuando describa su sugerencia. Si ha encontrado un error, por favor incluya el número de sección y parte del texto que rodea el error para que podamos encontrarlo más fácilmente.

Parte I. Requerimientos y limitaciones

Requerimientos del sistema, restricciones del soporte y limitaciones para la virtualización con Fedora

Los capítulos siguientes se concentran en los requerimientos del sistema, las restricciones del soporte y las limitaciones para la virtualización en Fedora.

Requerimientos del sistema

Este capítulo ofrece una lista con los requerimientos del sistema necesarios para poder realizar una virtualización exitosa en Fedora. La virtualización es posible en Fedora.

El hipervisor *Máquinas virtuales basadas en el Kernel* es ofrecido con Fedora.

Para obtener información sobre la instalación de los paquetes de virtualización, lea la *Capítulo 4, Instalación de paquetes virtuales*.

Requerimientos mínimos del sistema

- 6GB de espacio de disco libre
- 2GB de RAM

Requerimientos recomendados del sistema

- 6GB más el espacio de disco requerido por el sistema operativo por huésped. Para la mayoría de sistemas operativos se recomiendan más de 6GB de espacio libre.
- Un núcleo de procesador o hiper-hilo para cada CPU virtualizada y para e hipervisor.
- 2 GB de RAM, y RAM adicional para los huéspedes virtualizados.

Sobre envío de KVM

KVM tiene la posibilidad de sobreasignar recursos físicos para huéspedes virtualizados. Sobreasignar recursos significa que tanto la totalidad de la memoria RAM virtualizada como los núcleos del procesador utilizados por los huéspedes, pueden ser superiores a la cantidad de memoria RAM y a los núcleos del procesasor físicos del equipo. Para obtener más información sobre cómo sobreasignar recursos con KVM, consulte la *Sección 25.3, "Sobrealojamiento con KVM"*.

Requerimientos de KVM

El hipervisor KVM requiere:

- Un procesador Intel con las extensiones Intel VT e Intel 64 o
- Un procesador de AMD con extensiones AMD-V y AMD64.

Para determinar si su procesador tiene las extensiones de virtualización, consulte la *Sección 25.4, "Cómo verificar las extensiones de virtualización"*.

Soporte de almacenaje

Los métodos existentes de almacenamiento de huéspedes son:

- archivos en almacenaje local,
- particiones de discos duros físicos
- LUN físicamente conectados

- Particiones LVM,
- iSCSI, y
- LUNs basados canal de fibra.

Almacenamiento de huésped basado en archivo

Las imágenes de huéspedes basadas en archivo deberían en ser almacenadas en la carpeta **`/var/lib/libvirt/images/`**. Si se utiliza un directorio diferente, debe agregarlo a la política de SELinux. Para obtener mayor información, consulte la *Sección 19.2, "SELinux y virtualización completas"*.

Compatibilidad de KVM

El hipervisor KVM necesita un procesador con las extensiones de virtualización Intel-VT o AMD-V.

Tenga en cuenta que esta lista no se encuentra finalizada. Ayúdenos a completarla enviando un reporte de error con cualquier cosa que usted haya logrado hacer funcionar.

Para verificar si su procesar tiene soporte para las extensiones de virtualización, y para obtener información acerca de cómo habilitar estas extensiones llegado el caso que se encuentren deshabilitadas, diríjase a *Sección 25.4, “Cómo verificar las extensiones de virtualización”*.

El paquete de Fedora *kvm* se encuentra limitado a 256 núcleos de procesador.

Huéspedes que deberían funcionar

Sistema operativo	Nivel de funcionamiento
BeOS	Funcionó
Linux para empresas de Red Hat 3 x86	Optimizados con controladores para-virtualizados
Linux para empresas de Red Hat 4 x86	Optimizados con controladores para-virtualizados
Linux para empresas de Red Hat 4 AMD 64 e Intel 64	Optimizados con controladores para-virtualizados
Linux para empresas de Red Hat 5 x86	Optimizados con controladores para-virtualizados
Linux para empresas de Red Hat 5 AMD 64 e Intel 64	Optimizados con controladores para-virtualizados
Linux para empresas de Red Hat 6 x86	Optimizados con controladores para-virtualizados
Linux para empresas de Red Hat 6 AMD 64 e Intel 64	Optimizados con controladores para-virtualizados
Fedora 12 x86	Optimizados con controladores para-virtualizados
Fedora 12 AMD 64 e Intel 64	Optimizados con controladores para-virtualizados
Windows Server 2003 R2 32-Bit	Optimizados con controladores para-virtualizados
Windows Server 2003 R2 64-Bit	Optimizados con controladores para-virtualizados
Windows Server 2003 Service Pack 2 32-Bit	Optimizados con controladores para-virtualizados
Windows Server 2003 Service Pack 2 64-Bit	Optimizados con controladores para-virtualizados
Windows XP de 32 bits	Optimizados con controladores para-virtualizados
Windows Vista de 32 bits	Deberían funcionar
Windows Vista de 64 bits	Deberían funcionar
Windows Server 2000 de 32 bits	Optimizados con controladores para-virtualizados
Windows Server 2003 de 64 bits	Optimizados con controladores para-virtualizados
Windows 7 de 32 bits	Optimizados con controladores para-virtualizados
Windows 7 de 64 bits	Optimizados con controladores para-virtualizados

Sistema operativo	Nivel de funcionamiento
Open Solaris 10	Funcionó
Open Solaris 11	Funcionó

Limitaciones de virtualización

Este capítulo trata acerca de limitaciones adicionales de los paquetes de virtualización en Fedora

3.1. Limitaciones generales para virtualización

Otras limitaciones

Para conocer una lista con todas las demás limitaciones y problemas que afectan a la virtualización lea las *Notas del lanzamiento de Fedora 13*. En ellas se detallan las características actuales, los problemas y las limitaciones conocidas, aspectos que se van actualizando en la medida que van siendo descubiertos.

Lanzamiento antes de prueba

Debe probar con la máxima capacidad de carga anticipada y tensión de red virtualizado antes del lanzar aplicaciones pesadas de E/S. La prueba de tensión es importante porque hay bajas de rendimiento causadas por la virtualización con el uso aumentado de E/S

3.2. Limitaciones de KVM

Las siguientes limitaciones se aplican al hiperviso de KVM hipervisor:

Bit constante TSC
: Los sistemas que no poseen un contador de marca de tiempo constante necesitan una configuración adicional. Consulte el *Capítulo 17, Administración del tiempo del huésped KVM* para obtener mayor información y poder determinar si tiene o no un contador de marca de tiempo constante y los pasos de configuración a seguir para corregir problemas relacionados.

Sobre envío de memoria
: KVM soporta sobrecarga de memoria y puede almacenar la memoria de los huéspedes en swap. Un huésped se ejecutará más lento si es intercambiado con frecuencia. Cuando *KSM* es utilizado, asegúrese que el tamaño de swap sea proporcional al tamaño de la sobrecarga.

Sobrecarga de CPU
: No se recomienda tener más de 10 CPU virtuales por núcleo de procesador físico. Cualquier número de CPU virtuales sobrecargadas por encima del número de núcleos de procesador físicos, pueden presentar problemas con ciertos huéspedes virtualizados.

  La sobrecarga de CPUs tiene algunos riesgos y puede llevar a la inestabilidad. Consulte la *Sección 25.3, “Sobrealojamiento con KVM”* para obtener consejos y recomendaciones acerca de la sobrecarga en las CPUs.

Dispositivos virtualizados SCSI
: Las emulaciones SCSI se encuentran limitadas a 16 dispositivos SCSI virtualizados (emulados).

Dispositivos IDE virtualizados
: KVM está limitado a un máximo de cuatro dispositivos IDE (emulados) por huésped.

Controladores para-virtualizados
: Los dispositivos para-virtualizados, los cuales usan los controladores **`virtio`** son dispositivos de PCI. Actualmente, los huéspedes están limitados a un máximo de 32 dispositivos de PCI.

Algunos dispositivos de PCI son importantes para que el huésped se ejecute y estos dispositivos no pueden removerse. Los dispositivos predeterminados requeridos son:

- el puente de host,
- el puente ISA y el puente USB (Los puentes USB e ISA son el mismo dispositivo),
- la tarjeta gráfica (usando el controlador Cirrus o qxl) y
- el dispositivo de memoria de globo

De los 32 dispositivos PCI que se encuentran disponibles para un huésped, cuatro no son removibles. Esto significa para cada huésped existen disponibles solo 28 ranuras de PCI para dispositivos adicionales. Cada huésped puede utilizar hasta 28 dispositivos adicionales compuestos por cualquier tipo de combinación de redes para-virtualizadas, dispositivos de disco para-virtualizados, o cualquier otro dispositivo PCI que utilice VT-d.

Limitaciones de migración
: La migración en vivo es sólo posible con CPU del mismo proveedor (es decir, Intel a Intel o AMD a AMD únicamente).

  En una migración en vivo, el bit de No eXecution (NX, No ejecución) debe estar encendido (on) o apagado (off) para ambas CPU.

Limitaciones de almacenamiento
: El euipo no debería utiizar etiquetas de disco para identificar sistemas de archivos en los archivos **`fstab`**, **`initrd`**, o algún otro utilizado en la línea de comando del kernel. Si los usuarios con nivel de autorización bajo (especialmente los huéspedes virtualizados) tuvieran acceso a todas las particiones, o a volúmenes LVM, el sistema del equipo anfitrión podría verse comprometido.

  Los huéspedes no deberían tener acceso de escritura a la totalidad del disco, o a los dispositivos de bloques (como por ejemplo, **`/dev/sdb`**. Los huéspedes virtualizados con acceso a ciertos dispositivos de bloques, podrían ser capaces de acceder a dispositivos de bloques del sistema, o modificar etiquetas de volúmenes que podrían ser utilizadas para comprometerlo. Utilice particiones (por ejemplo **`/dev/sdb1`**), o volúmenes lógicos para evitar este tipo de inconvenientes.

Llimitaciones de PCI passthrough
: Asociar dispositivos PCI a los huéspedes (PCI passthrough) debería funcionar en sistemas con tecnologías AMD IOMMU, o Intel VT-d

3.3. Limitaciones de aplicación

Hay aspectos de virtualización que pueden hacer la virtualización no apta para algunos tipos de aplicaciones.

La aplicaciones con requerimientos de rendimiento de E/S, deben utilizar los controladores para-virtualizados para huéspedes completamente virtualizados. Sin los controladores para-virtualizados algunas aplicaciones pueden ser inestables bajo cargas pesadas de E/S.

Las siguientes aplicaciones deben evitarse por sus amplias razones de requerimientos de E/S

- servidor **kdump**
- servidor **netdump**

Se deben evaluar cuidadosamente las aplicaciones de bases de datos antes de ejecutarlas en un huésped virtualizado. Las bases de datos generalmente utilizan de modo intenso E/S de dispositivos de red y de almacenamiento. Estas aplicaciones podrían no ser aptas en un entorno completamente virtualizado. Considere una para-virtualización o los dispositivos para-virtualizados para desempeño aumentado de E/S. Consulte el *Capítulo 12, Controladores KVM para-virtualizados* para obtener mayor información acerca de controladores para-virtualizados para invitados completamente virtualizados.

También deben evaluarse cuidadosamente otras aplicaciones y herramientas que utilcen mucho la E/S, o que necesiten de un rendimiento de tiempo real. El uso de virtualización completa con controladores para-virtualizados (consulte el *Capítulo 12, Controladores KVM para-virtualizados*), o direfctamente la utilización de para virtualización, produce un mejor rendimiento con aplicaciones de E/S intensiva. De todos modos, las aplicaciones sufren una pequeña pérdida de su rendimiento al ser ejecutadas en entornos virtualizados. Los posibles beneficios del rendimiento de una virtualización consolidada sobre un hardware rápido y reciente, deben ser evaluados con respecto a los posibles problemas de rendimiento de la aplicación, asociados a la utilización de hardware completamente virtualizado.

Parte II. Instalación

Temas de instalación de virtualización

Estos capítulos describen la configuración del anfitrión y la instalación de huéspedes virtualizados con Fedora. Se recomienda leer estos capítulos detenidamente para asegurar una instalación exitosa de los sistemas operativos huéspedes virtualizados.

Instalación de paquetes virtuales

Antes de que pueda utilizar la virtualización, los paquetes necesarios para ello tienen que haber sido instaladosen su computadora. Estos paquetes pueden instalarse o bien durante la primera instalación de Fedora, o bien luego de haber finalizado dicho proceso, utilizando el comando **yum**, y la red de Red Hat (RHN, por las iniciales en inglés de Red Hat Network).

El hipervisor KVM utiliza el kernel predeterminado de Fedora con el módulo *kvm*.

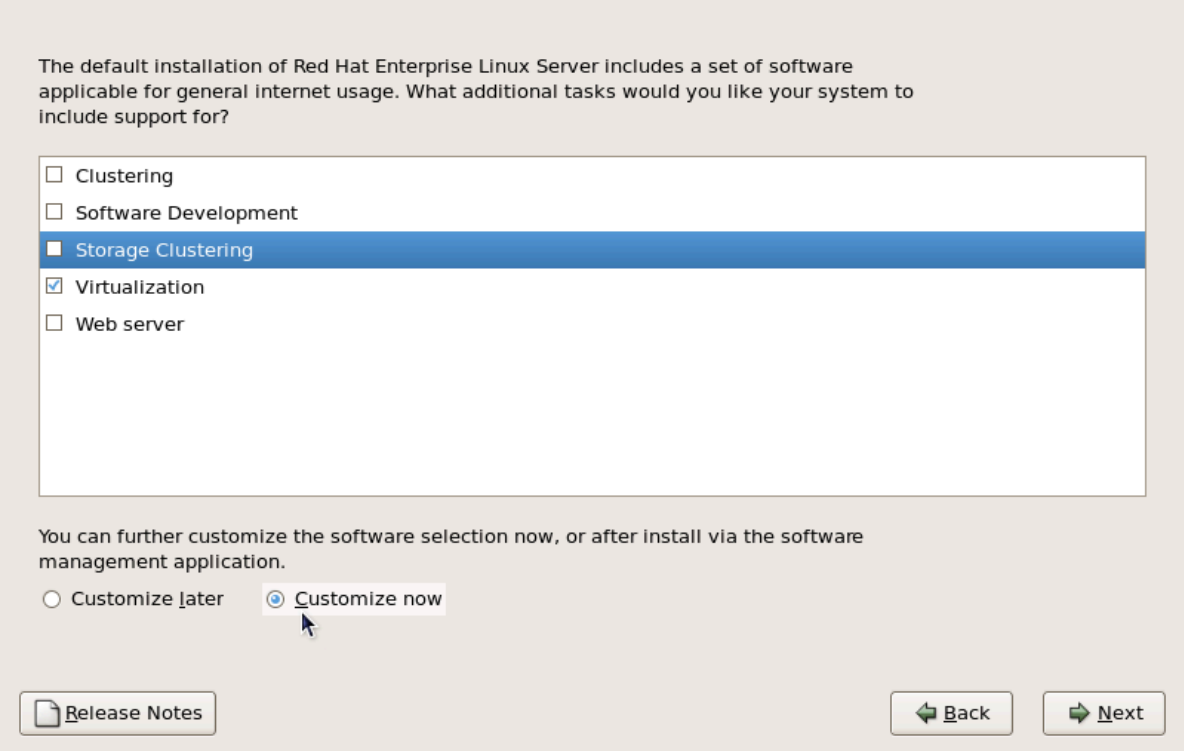
4.1. Instalación de KVM con instalación nueva de Fedora

Esta sección describe las herramientas de instalación y el paquete KVM, como parte de una instalación nueva de Fedora.

¿Necesita ayuda en la instalación?

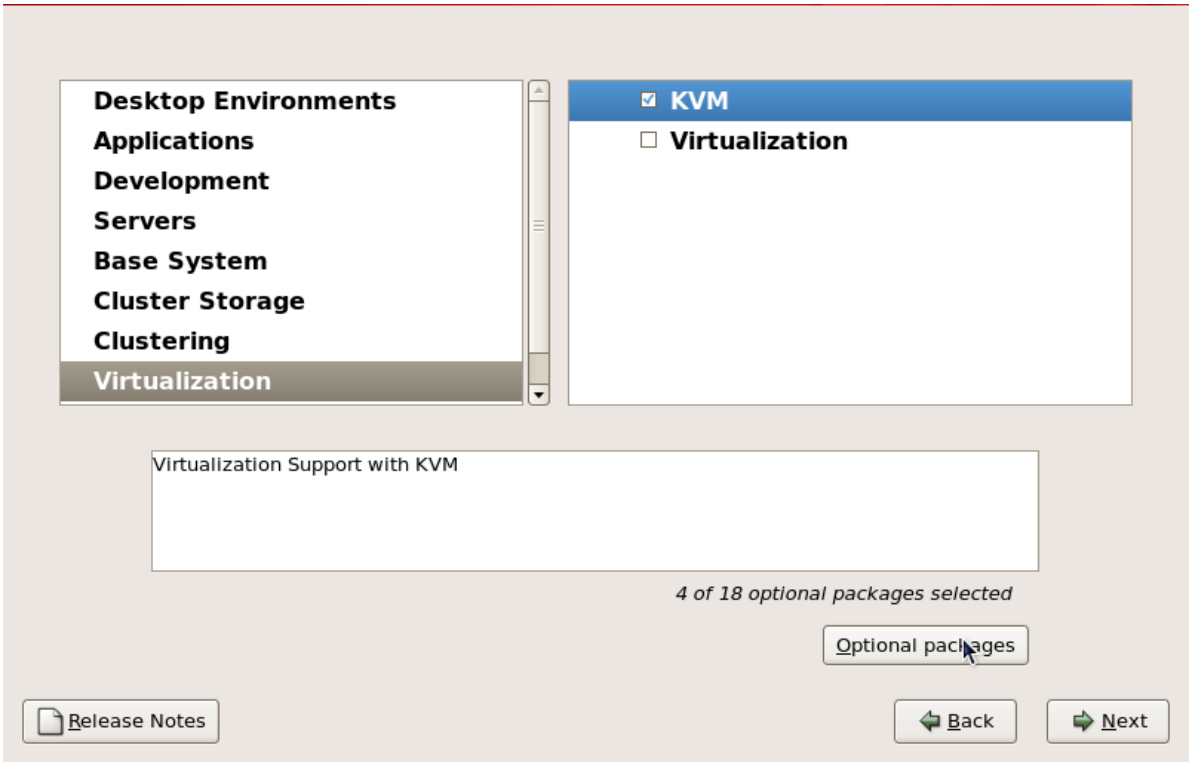
La *Guía de instalación de Fedora 13* (disponible en *http://docs.fedoraproject.org*) describe en detalle la instalación de Fedora.

1. Inicie una instalación interactiva de Fedora desde su CD-ROM, DVD o PXE de instalación.
2. Cuando le sea solicitado, debe ingresar un número válido de instalación para poder recibir acceso a la virtualización, y otros paquetes de Plataformas avanzadas.
3. Complete los demás pasos hasta el paso de la selección de paquetes.

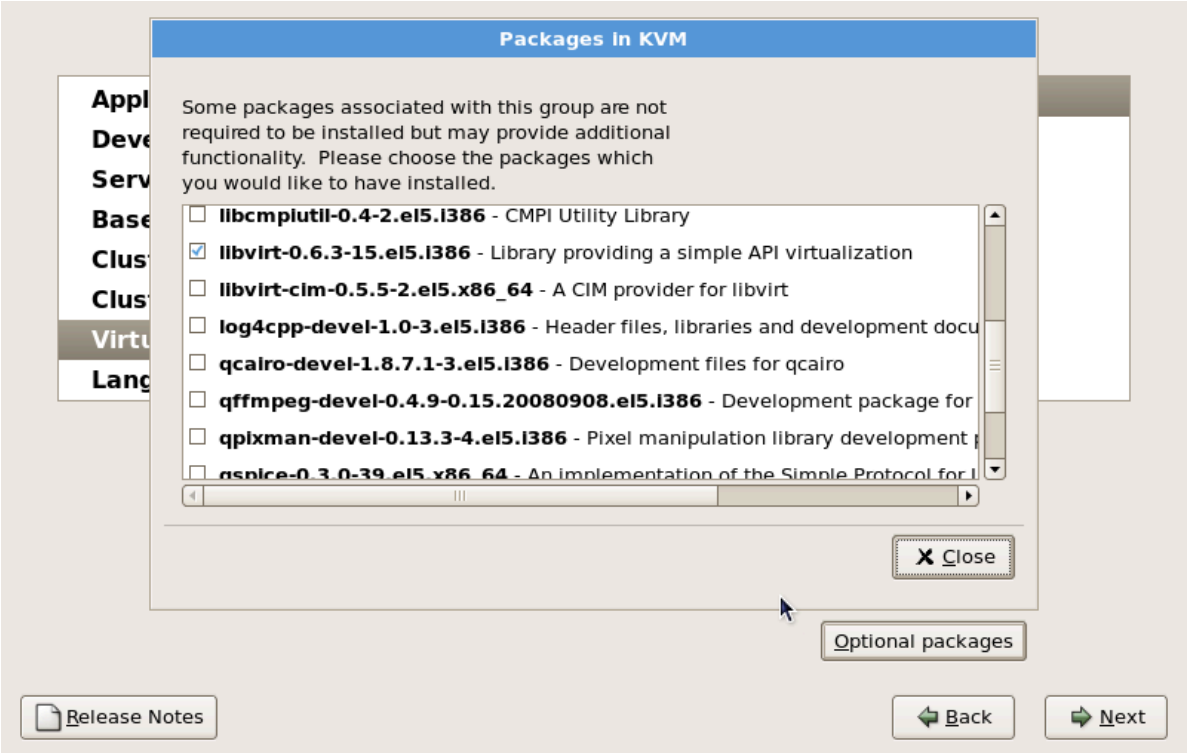

The default installation of Red Hat Enterprise Linux Server includes a set of software applicable for general internet usage. What additional tasks would you like your system to include support for?
Clustering
Software Development
Storage Clustering
Virtualization
Web server
You can further customize the software selection now, or after install via the software management application.
Customize later
Customize now
Release Notes
Back
Next

Seleccione el grupo de paquete **Virtualización** y el botón **Personalizar ahora**.

4. Seleccione el grupo de paquete **KVM**. Desactive el grupo de paquete **Virtualización**. Éste selecciona el hipervisor KVM, **`virt-manager`**, **`libvirt`** y **`virt-viewer`** para instalación.



5. **Personalizar los paquetes (si se requiere)**
Personalizar el grupo de **Virtualización** si requiere otros paquetes de virtualización.


Packages in KVM
Some packages associated with this group are not required to be installed but may provide additional functionality. Please choose the packages which you would like to have installed.
libcmpiutil-0.4-2.el5.i386 - CMPI Utility Library
libvirt-0.6.3-15.el5.i386 - Library providing a simple API virtualization
libvirt-cim-0.5.5-2.el5.x86_64 - A CIM provider for libvirt
log4cpp-devel-1.0-3.el5.i386 - Header files, libraries and development docu
qcairo-devel-1.8.7.1-3.el5.i386 - Development files for qcairo
qffmpeg-devel-0.4.9-0.15.20080908.el5.i386 - Development package for
qpixman-devel-0.13.3-4.el5.i386 - Pixel manipulation library development
Close
Optional packages
Release Notes
Back
Next

Presione los botónes de **Cerrar** seguido de **Siguiente** para continuar la instalación.

Instalación de paquetes KVM con archivos Kickstart

Esta sección describe cómo utilizar un archivo Kickstart para instalar Fedora con los paquetes de hipervisor KVM. Los archivos Kickstart permiten grandes instalaciones automatizadas desatendidas sin necesidad de que el usuario instale cada sistema individual. Los pasos en esta sección le ayudarán en la creación y uso de un archivo Kickstart para instalar Fedora con los paquetes de virtualización.

En la sección **%packages**de su archivo Kickstart, añada el siguiente grupo de paquete:

```
%packages
@kvm
```

Puede encontrarse mayor información relacionada con los archivos Kickstart en la *Guía de instalación de Fedora 13*, disponible en *http://docs.fedoraproject.org*.

4.2. Instalación de paquetes KVM en un sistema Fedora existente

Esta sección describe los pasos para poder instalar el hipervisor KVM en un sistema Fedora que ya esté funcionando, o en uno nuevo.

Instalación del hipervisor KVM con yum

Para poder utilizar la virtualización con Fedora es necesario el paquete **kvm**. Este paquete contiene el módulo de kernel de KVM, que proporciona el hipervisor KVM, sobre el kernel predeterminado de Fedora.

Para instalar el paquete **kvm**, ejecute:

```
# yum install kvm
```

Ahora, instale los paquetes adicionales de administración de virtualización.

Paquetes de virtualización recomendados:

python-virtinst

Proporciona el comando **virt-install** para crear máquinas virtuales.

libvirt

libvirt es una Interfaz de aplicación de programadores multiplataforma (API, por las iniciales en inglés de Application Programmers Interface) que permite interactuar con los sistemas del hipervisor y del equipo. *libvirt* administra los sistemas y controla el hipervisor. El paquete *libvirt* ofrece la herramienta de línea de comando **virsh** para administrar y controlar huéspedes virtualizados e hipervisores, o bien desde la línea de comando, o bien desde una shell de virtualización especial.

libvirt-python

El paquete *python-virtinst* contiene un módulo que permite que las aplicaciones escritas en el lenguaje de programación Python, puedan utilizar la interfaz proporcionada por la API de **libvirt**.

virt-manager

`virt-manager`, también conocido como el **Administrador de máquina virtual**, proporciona una herramienta gráfica para administrar máquinas virtuales. Utiliza la biblioteca *libvirt* como la API de administración.

Instale los otros paquetes de virtualización recomendados:

```
# yum install virt-manager libvirt libvirt-python python-virtinst
```

Introducción a la instalación de un huésped virtualizado

Después de haber instalado los paquetes de virtualización en el sistema de host, puede crear sistemas operativos de huésped. Este capítulo describe los procesos generales para la instalación de sistemas operativos de huésped en máquinas virtuales. Puede crear huéspedes con el botón **Nuevo** en **virt-manager** o utilizar la interfaz de línea de comandos **`virt-install`**. Ambos métodos se describen en este capítulo.

Existen disponibles instrucciones de instalación más detalladas para versiones específicas de Fedora, otras distribuciones Linux, Solaris y Windows. Diríjase al procedimiento adecuado de acuerdo a su sistema operativo:

- Linux para empresas de Red Hat 5: *Capítulo 6, Cómo instalar Linux para empresas de Red Hat 5 como un huésped completamente virtualizado*
- Windows XP: *Capítulo 7, Instalación de Windows XP como huésped completamente virtualizado*
- Windows Server 2003: *Capítulo 8, Instalación de Windows Server 2003 como un huésped completamente virtualizado*
- Windows Server 2008: *Capítulo 9, Installing Windows Server 2008 como huésped totalmente virtualizado*

5.1. Consideraciones y pre requisitos relacionados con los huéspedes virtualizados

Antes de pensar en crear cualquier tipo de huésped virtualizado, deberían considerarse algunos factores. Entre ellos:

- Desempeño
- Requerimientos y tipos de entrada/salida
- Almacenamiento
- Entorno e infraestructura de la red

Desempeño

La virtualización tiene un impacto en el desempeño.

Requerimientos y arquitecturas de E/S

.

Almacenamiento

.

Entorno e infraestructura de la red

.

5.2. Creación de huéspedes con virt-install

Puede utilizar **virt-install** para crear huéspedes virtualizados desde la línea de comando. **virt-install**, ya sea de forma interactiva o como parte de un script para automatizar la creación de las máquinas virtuales. El uso de **virt-install** con archivos Kickstart files permite una instalación de máquinas virtuales sin supervisión.

La herramienta **virt-install** proporciona un número de opciones que se pueden pasar a la línea de comandos. Para ver una lista completa de opciones ejecute:

```
$ virt-install --help
```

La página man **virt-install** también documenta cada opción de comando y variables importantes.

El comando **qemu-img** es un comando que puede utilizarse antes de **virt-install** para configurar opciones de almacenaje.

An important option is the *--vnc* option which opens a graphical window for the guest's installation.

Este ejemplo crea un huésped de Red Hat Enterprise Linux 3, llamado *rhel3support*, desde un CD-ROM, con redes virtuales y con un archivo de 5GB basado en imagen de dispositivo de bloque. Este ejemplo utiliza el hipervisor de KVM.

```
# virt-install --accelerate --hvm --connect qemu:///system \
   --network network:default \
   --name rhel3support --ram=756\
   --file=/var/lib/libvirt/images/rhel3support.img \
   --file-size=6 --vnc --cdrom=/dev/sr0
```

Ejemplo 5.1. Uso de virt-install con KVM para crear un huésped de Red Hat Enterprise Linux 3

```
# virt-install --name fedora11 --ram 512 --file=/var/lib/libvirt/images/fedora11.img \
 --file-size=3 --vnc --cdrom=/var/lib/libvirt/images/fedora11.iso
```

Ejemplo 5.2. Cómo utilizar virt-install para crear un huésped de fedora 11

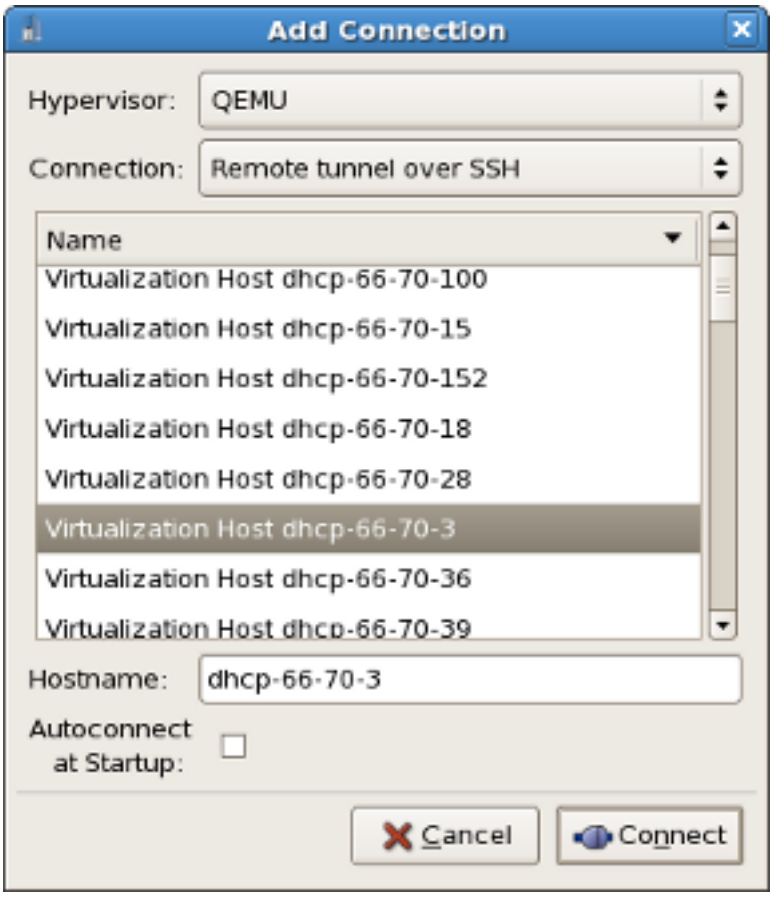
5.3. Creación de huéspedes con virt-manager

virt-manager, también conocido como un Administrador de máquina virtual es una herramienta gráfica para crear y administrar los huéspedes virtualizados.

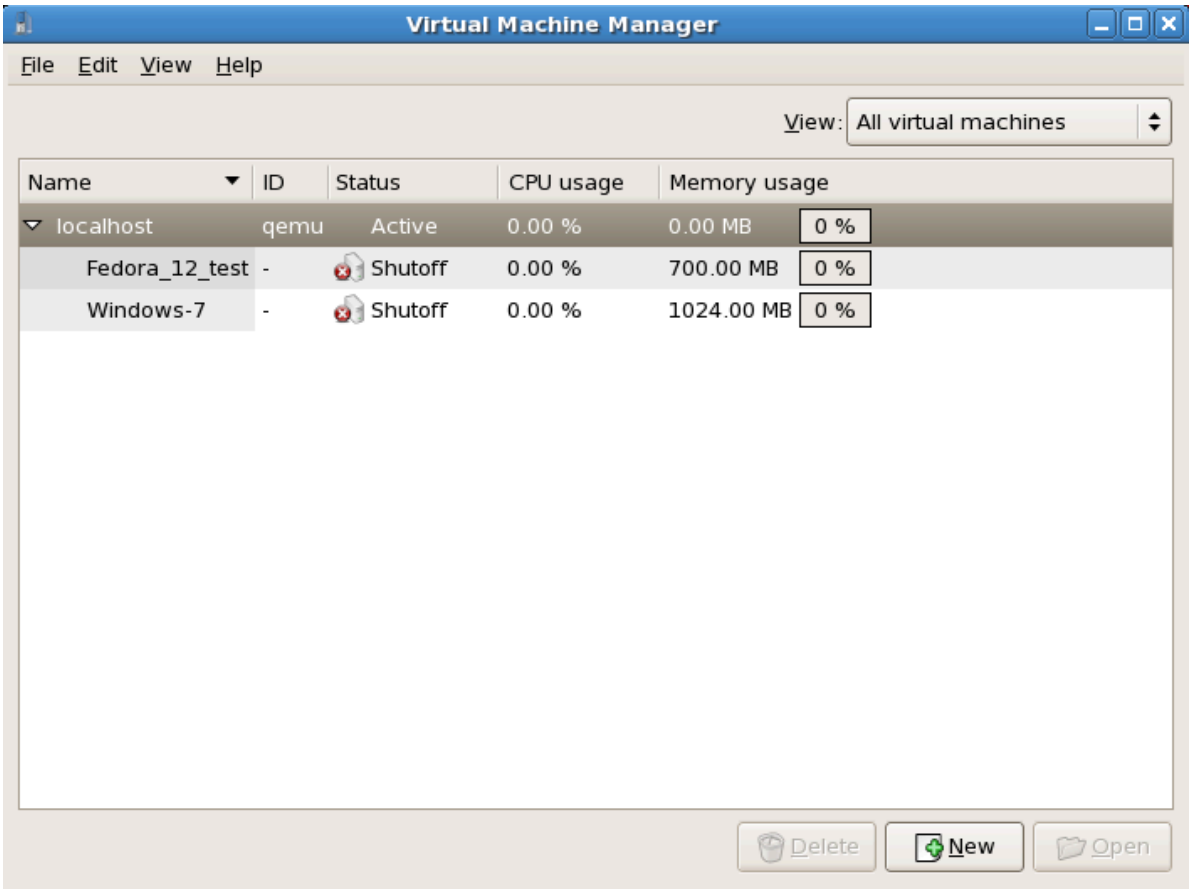
Procedimiento 5.1. Creación de un huésped virtualizado con **virt-manager**

1. **Inicie virt-manager**
   Inicie **virt-manager**: Lance la aplicación **Virtual Machine Manager** desde el menú **Aplicaciones** y del submenú **Herramientas del sistema**. De forma alternativa, ejecute el comando **virt-manager**

2. **Opcional: Abra un hipervisor remoto**
   Open the **File -> Add Connection**. The dialog box below appears. Select a hypervisor and click the **Connect** button:



3. **Crear un nuevo huésped**
   La ventana **virt-manager** le permite crear una nueva máquina virtual. Haga clic en el botón **Nuevo** para crear un nuevo huésped. De esta manera se abre el asistente como se muestra en la instantánea.


Virtual Machine Manager
File Edit View Help
View: All virtual machines
Name ID Status CPU usage Memory usage
localhost qemu Active 0.00 % 0.00 MB 0 %
Fedora_12_test - Shutoff 0.00 % 700.00 MB 0 %
Windows-7 - Shutoff 0.00 % 1024.00 MB 0 %
Delete New Open

4. **Asistente de nuevo huésped**
   La ventana **Crear una nueva máquina virtual** proporciona un resumen de la información que usted debe indicar para crear una máquina virtual:

Create a new virtual machine
Virtual Machine Creation
This assistant will guide you through creating a new virtual machine. You will be asked for some information about the virtual machine you'd like to create, such as:
A name for your new virtual machine
Whether the virtual machine will be fully virtualized or para-virtualized
The location of the files necessary for installing an operating system on the virtual machine
Storage details - which disk partitions or files the virtual machine should use
Memory and CPU allocation
Cancel
Back
Forward

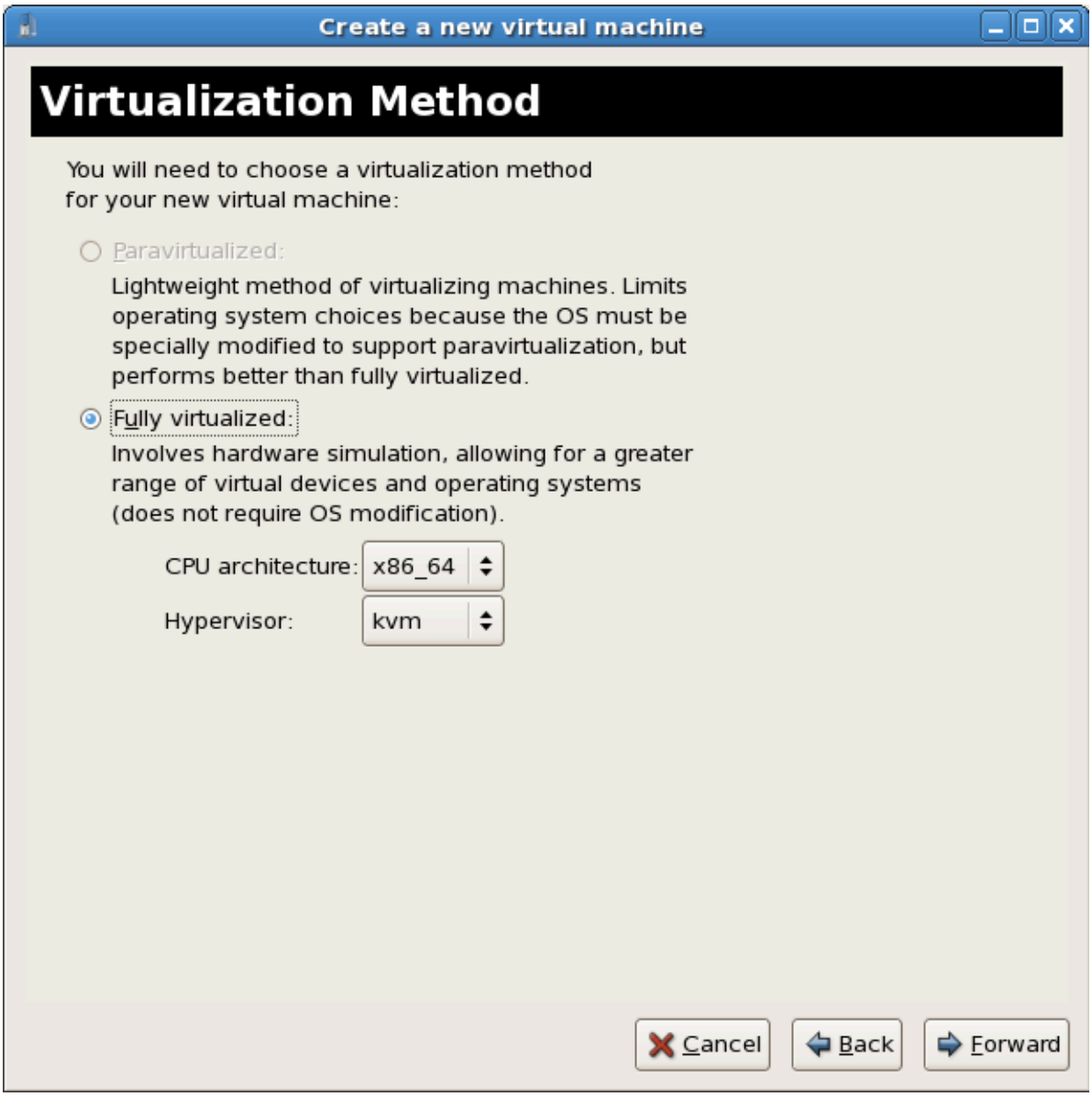
Revise la información para su instalación y haga clic en el botón **Adelante**.

5. **Indique un nombre para la máquina virtual**
   The following characters are allowed in guest names: '_', '**.**' and '**-**' characters.

Presione **Forward** para continuar.

6. **Elija un método de virtualización**
   Aparece la ventana de **Seleccionar un método de virtualización**.

   Una virtualización completa necesita un procesador con las extensiones AMD 64 y AMD-V, o de un procesador con las extensiones Intel 64 e Intel VT. Si estas extensiones de virtualización no están presentes, KVM no estará disponible.


Create a new virtual machine
Virtualization Method
You will need to choose a virtualization method
for your new virtual machine:
Paravirtualized:
Lightweight method of virtualizing machines. Limits
operating system choices because the OS must be
specially modified to support paravirtualization, but
performs better than fully virtualized.
Fully virtualized:
Involves hardware simulation, allowing for a greater
range of virtual devices and operating systems
(does not require OS modification).
CPU architecture: x86_64
Hypervisor: kvm
Cancel
Back
Forward

Elija el tipo de virtualización y haga clic en el botón **Siguiente**.

7. **Seleccion el el método de instalación**
   La ventana de **Método de instalación** le pregunta por el tipo de virtualización que ha seleccionado.

   Los huéspedes pueden ser instalados utilizando uno de los siguientes métodos:

   Medio de instalación local
   : Este método utiliza un CD-ROM, o un DVD, o una imagen de instalación en CD-ROM o DVD, (un archivo **`.iso`**).

   Arbol de instalación de red
   : Este método utiliza un espejo de un árbol de instalación de Fedora para instalar huéspedes. Debe accederse a este árbol de instalación utilizando alguno de los siguientes protocolos de red: HTTP, FTP, o NFS.

Los archivos y servicios de red pueden ser alojados utilizando servicios de red en el equipo, o en otro espejo.

Arranque de red

Este método utiliza un Entrono de ejecución de prearranque (PXE, por las iniciales en inglés de Preboot eXecution Environment) para instalar el huésped. La configuración de un servidor PXE se detalla en la *Guía de despliegue de Fedora*. Utilizar este método necesita de un huésped con una dirección IP enrutable o un dispositivo de red compartido. Diríjase a *Capítulo 11, Configuración de la red* para obtener información acerca la configuración de red necesaria para una instalación PXE.

Create a new virtual machine
Installation Method
Please indicate where installation media is available for the operating system you would like to install on this virtual machine:
Local install media (ISO image or CDROM)
Network install tree (HTTP, FTP, or NFS)
Network boot (PXE)
Please choose the operating system you will be installing on the virtual machine:
OS Type: Generic
OS Variant: Generic
Not all operating system choices are supported by Red Hat. Please see the link below for supported configurations:
Red Hat Enterprise Linux 5 virtualization support
Cancel
Back
Forward

Defina el **tipo de SO** y la **variable del SO**.

Elija el método de instalación y haga clic en el botón **Siguiente** para continuar.

8. **Selección del medio de instalación**
   Esta ventana es dependiente de la elección que haya realizado en el paso anterior.

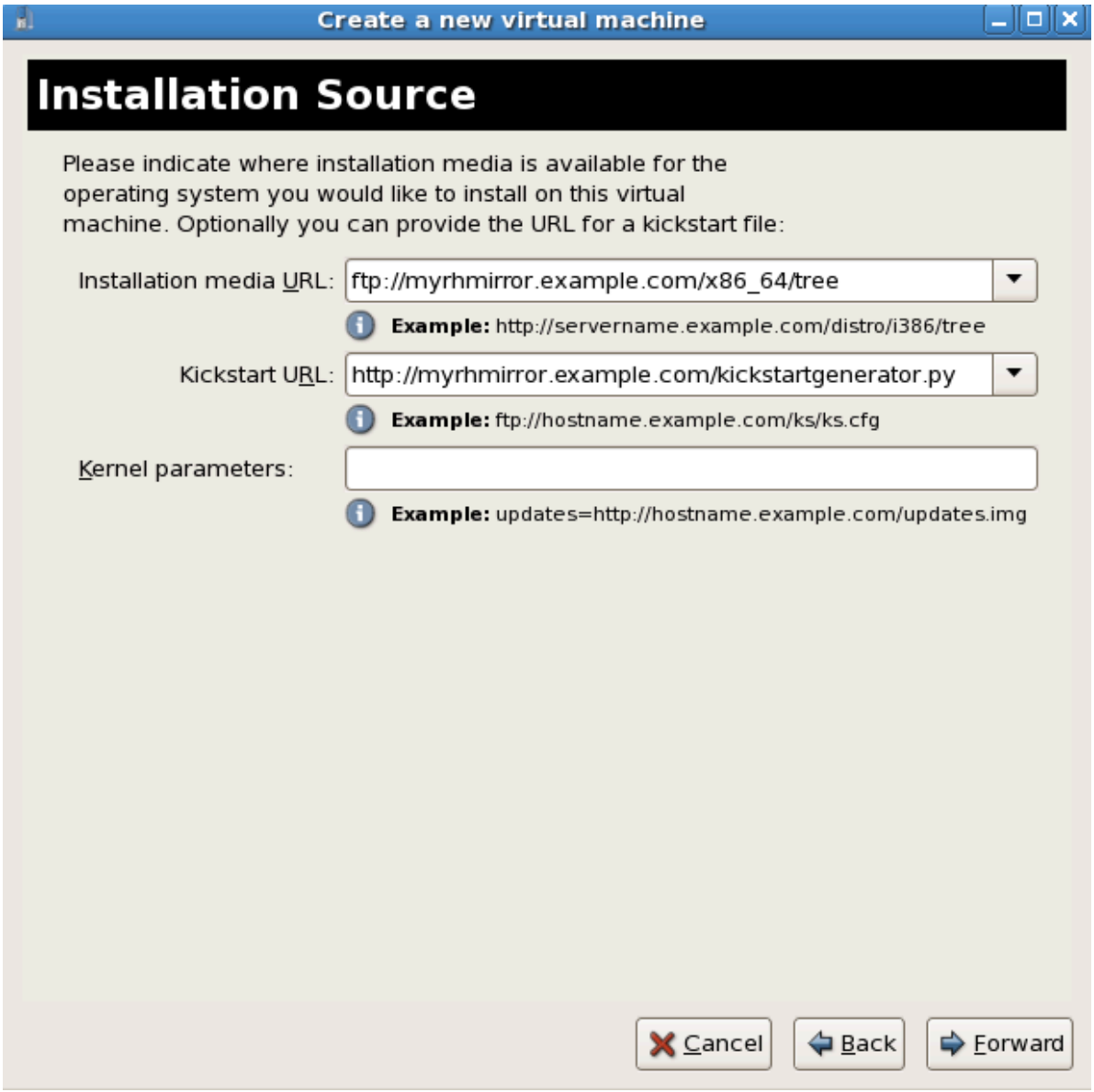
a. **Imagen ISO o medio de instalación físico**
Si se ha seleccionado **Medio de instalación local** en el paso anterior, esta pantalla será denominada **Medio de instalación**.

Seleccione la ubicación de un archivo de imagen ISO, o seleccione un CD-ROM o DVD desde la lista desplegable.

Haga clic en el botón **Adelante** para continuar.

b. **Instalación de un Arbol de instalación de red**
Si se ha seleccionado **Arbol de instalación de red** en el paso anterior, esta pantalla será denominada **Fuente de instalación**.

Una instalación de red necesita la dirección de un espejo de un árbol de instalación de Linux utilizando `NFS`, `FTP` o `HTTP`. De manera opcional, un archivo kickstart puede ser especificado para automatizar la instalación. Si es necesario, también pueden especificarse parámetros del Kernel.



Haga clic en el botón **Adelante** para continuar.

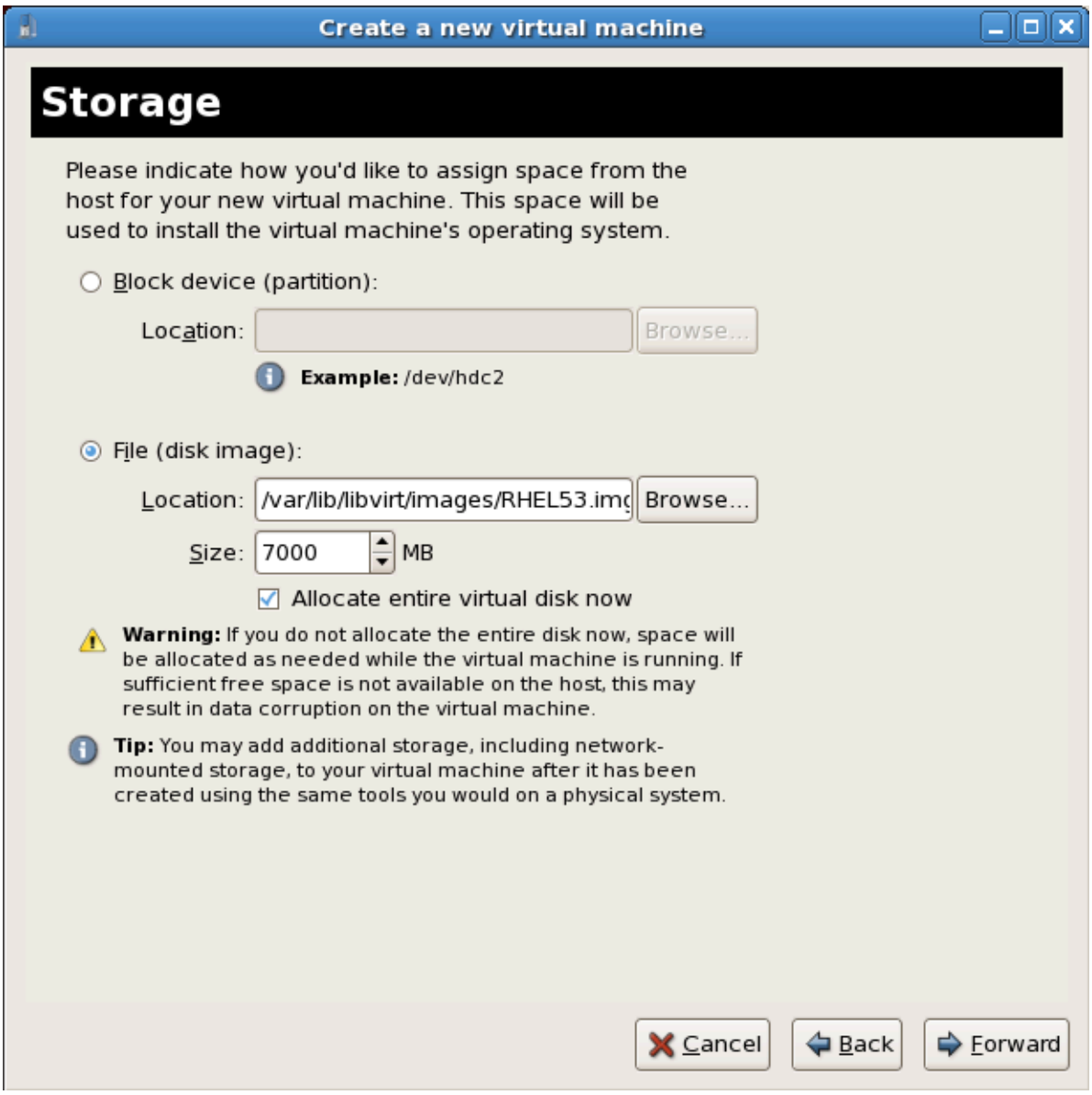
c. **Arranque de red (PXE)**
Una instalación PXE no posee un paso adicional.

9. **Configuración del almacenamiento**
Se muestra la ventana de **Almacenamiento**. Elija una partición de disco, LUN, o cree una imagen basada en un archivo para el huésped.

Todos los archivos de imagen deberían ser almacenados en el directorio **`/var/lib/libvirt/images/`**. Cualquier otra ubicación está prohibida por SELinux. Si ejecuta SELinux en modo impositivo, consulte la *Sección 19.2, "SELinux y virtualización completas"* para obtener mayor información acerca de la instalación de huéspedes.

Your guest storage image should be larger than the size of the installation, any additional packages and applications, and the size of the guests swap file. The installation process will choose the size of the guest's swap based on size of the RAM allocated to the guest.

Aloje espacio extra si el huésped necesita espacio adicional para aplicaciones u otros datos. Por ejemplo, los servidores web necesitan espacio adicional para los archivos de registro.


Create a new virtual machine
Storage
Please indicate how you'd like to assign space from the host for your new virtual machine. This space will be used to install the virtual machine's operating system.
Block device (partition):
Location:
Browse...
Example: /dev/hdc2
File (disk image):
Location:
/var/lib/libvirt/images/RHEL53.img
Browse...
Size:
7000
MB
Allocate entire virtual disk now
Warning: If you do not allocate the entire disk now, space will be allocated as needed while the virtual machine is running. If sufficient free space is not available on the host, this may result in data corruption on the virtual machine.
Tip: You may add additional storage, including network-mounted storage, to your virtual machine after it has been created using the same tools you would on a physical system.
Cancel
Back
Forward

Elija el tamaño apropiado para el huésped en el dispositivo de almacenamiento elegido y haga clic en el botón **Adelante**.

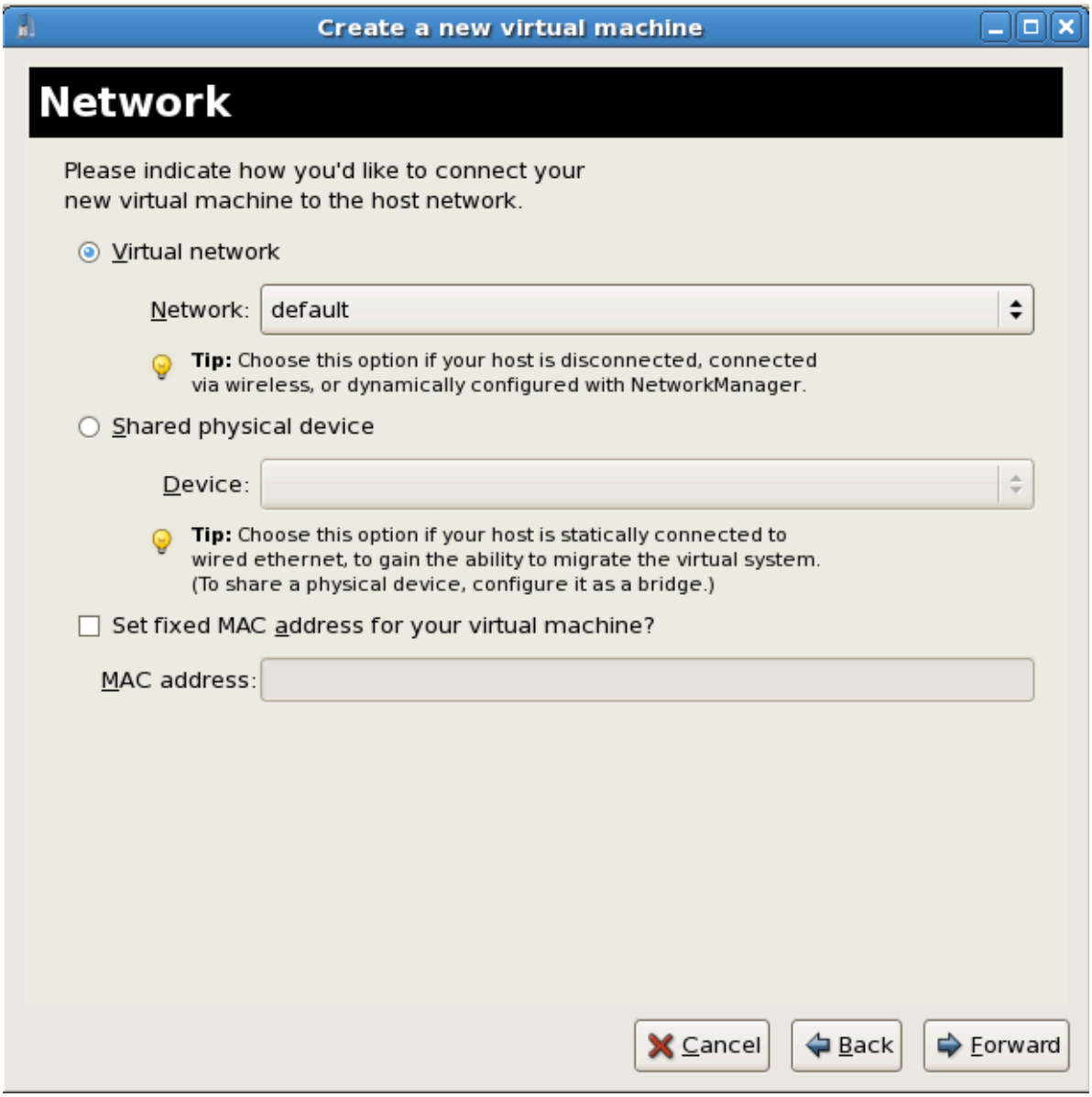
Nota

Se recomienda utilizar el directorio predeterminado para imágenes de máquinas virtuals, **`/var/lib/libvirt/images/`**. Si está utilizando una ubicación diferente (como lo es **`/images/`** en este ejemplo) asegúrese que sea añadido a su política de SELinux, y vuelva a etiquetarlo antes de continuar con la instalación (más adelante en este mismo documento encontrará cómo modificar su política de SELinux).

10. **Configuración de la red**
    Seleccione o bien **Red virtual**, o bien **Dispositivo físico compartido**.

    La opción de red virtual utiliza el protocolo de Traducción de dirección de red (NAT, por las iniciales en inglés de Network Address Translation) para compartir el dispositivo de red predeterminado con los huéspedes virtualizados. Utilice la opción de red virtual para redes inalámbricas.

    La opción de compartir dispositivo físico utiliza un enlace para poder ofrecerle al huésped virtualizado, un acceso total al dispositivo de red.

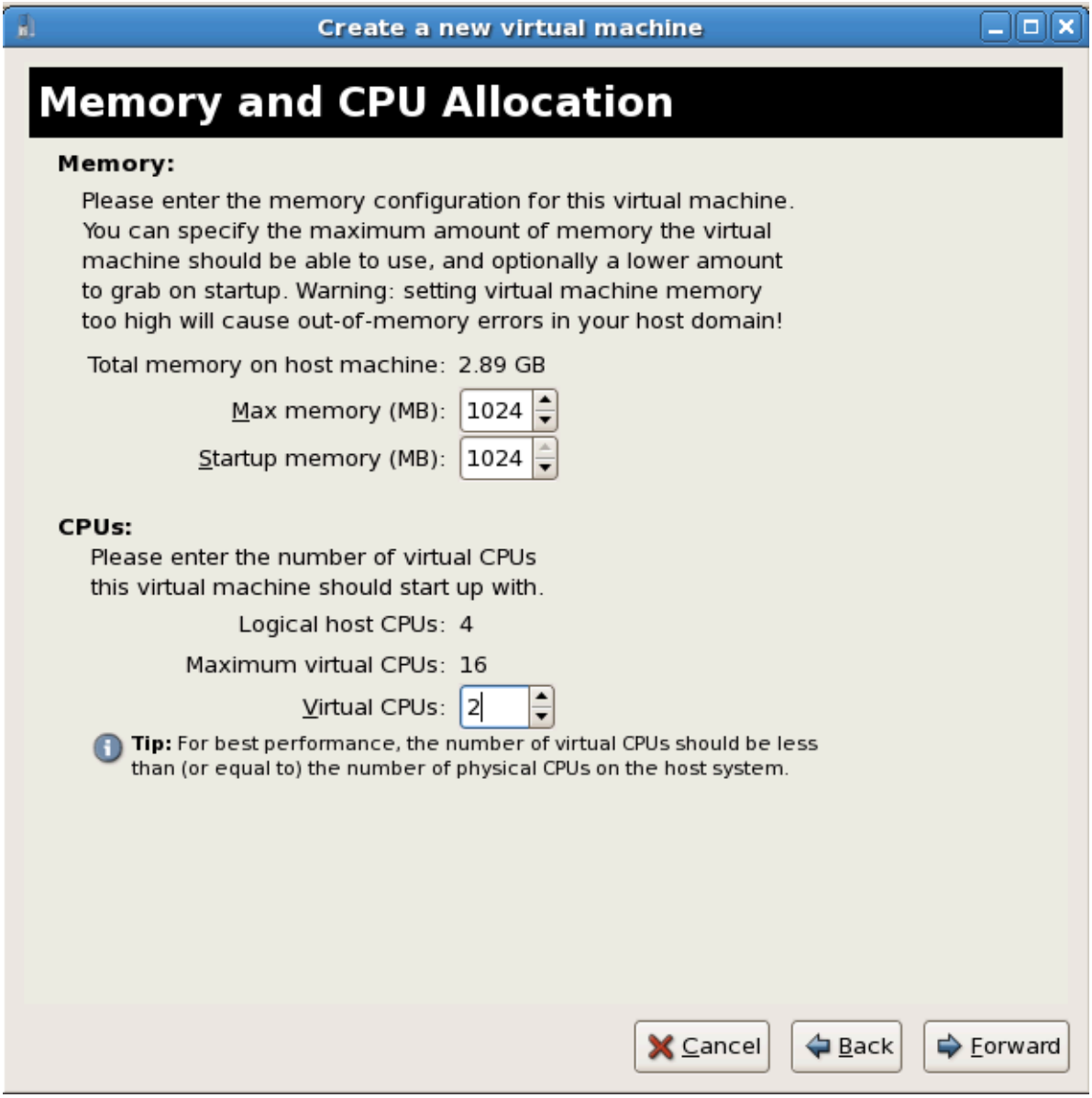

Create a new virtual machine
Network
Please indicate how you'd like to connect your new virtual machine to the host network.
Virtual network
Network: default
Tip: Choose this option if your host is disconnected, connected via wireless, or dynamically configured with NetworkManager.
Shared physical device
Device:
Tip: Choose this option if your host is statically connected to wired ethernet, to gain the ability to migrate the virtual system. (To share a physical device, configure it as a bridge.)
Set fixed MAC address for your virtual machine?
MAC address:
Cancel
Back
Forward

    Presione **Avanzar** para continuar.

11. **Alojamiento de la memoria y del CPU**
    The **Memory and CPU Allocation** window displays. Choose appropriate values for the virtualized CPUs and RAM allocation. These values affect the host's and guest's performance.

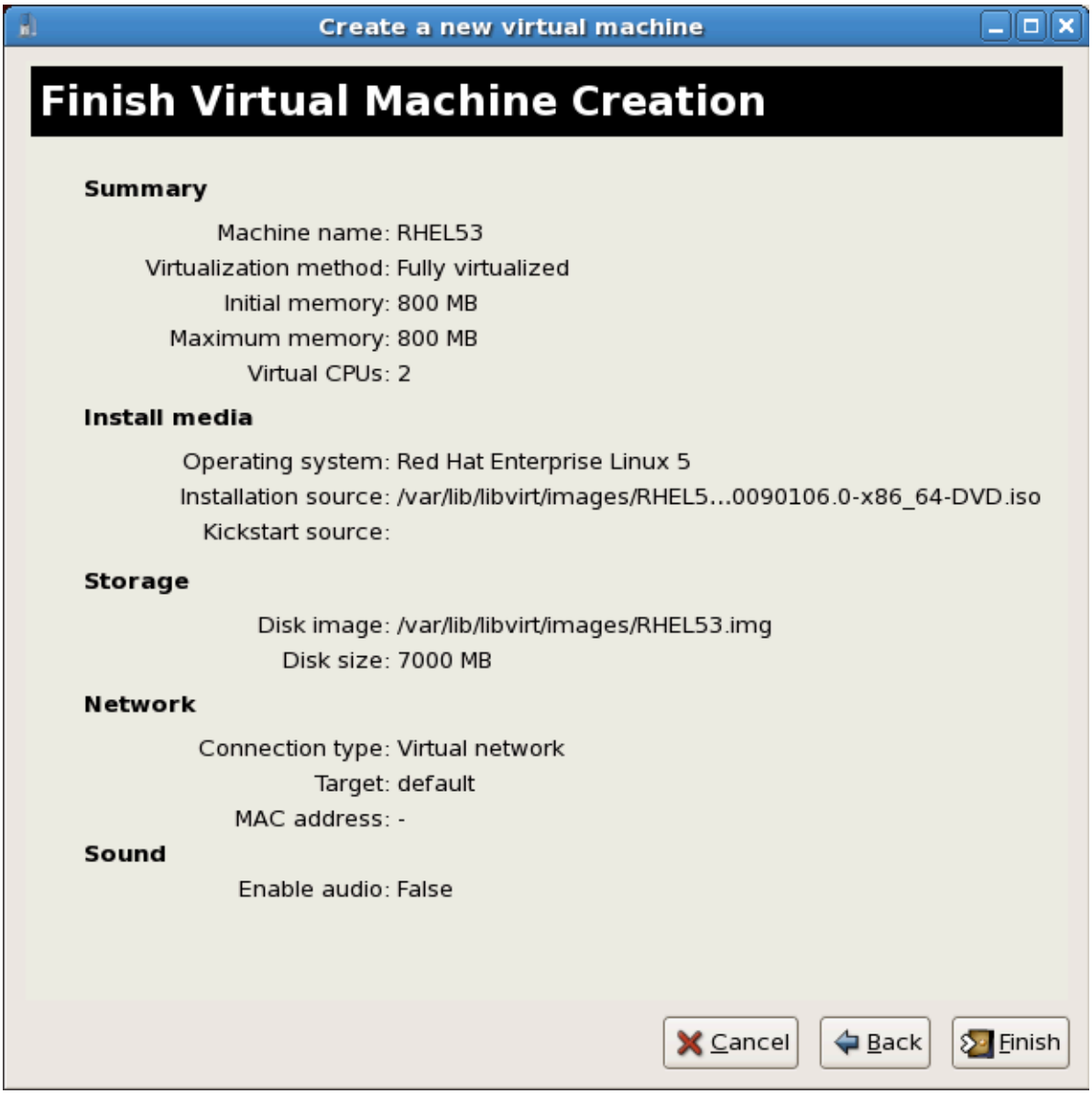
Los huéspedes requieren suficiente memoria física (RAM) para ejecutarse de modo eficiente y efectivo. Elija el valor de memoria que se ajuste a su sistema operativo de huésped y a los requerimientos de aplicación. La mayoría de los sistemas operativos requieren al menos 512MB de RAM para funcionar con receptividad. Recuerde, los huéspedes utilizan RAM física. La ejecución de muchos huéspedes o dejar memoria insuficiente para el sistema de host, resulta en un uso importante de memoria virtual. La memoria virtual es bastante lenta lo que produce un rendimiento de sistema y receptividad degradados. Asegúrese de asignar memoria suficiente a todos los huéspedes y al host para que funcionen de modo efectivo.

Asigne suficientes CPUs virtuales para el huésped virtualizado. Si el huésped ejecuta una aplicación múltiple, asigne la cantidad necesaria de CPUs virtuales que necesite el huésped para funcionar eficientemente. No asigne más CPUs virtuales que la cantidad de procesadores físicos disponibles en el sistema del equipo anfitrión. Si bien es posible sobre-alojar procesadores virtuales, el sobrealojamiento tiene un efecto significante y negativo en el desempeño tanto del huésped como del equipo, debido a los procesos generales del contexto de intercambio.


Create a new virtual machine
Memory and CPU Allocation
Memory:
Please enter the memory configuration for this virtual machine. You can specify the maximum amount of memory the virtual machine should be able to use, and optionally a lower amount to grab on startup. Warning: setting virtual machine memory too high will cause out-of-memory errors in your host domain!
Total memory on host machine: 2.89 GB
Max memory (MB): 1024
Startup memory (MB): 1024
CPUs:
Please enter the number of virtual CPUs this virtual machine should start up with.
Logical host CPUs: 4
Maximum virtual CPUs: 16
Virtual CPUs: 2
Tip: For best performance, the number of virtual CPUs should be less than (or equal to) the number of physical CPUs on the host system.
Cancel
Back
Forward

Presione **Forward** para continuar.

12. **Verificar e Iniciar la instalación del huésped**
    La ventana de **Finalizar la creación de la máquina virtual** le ofrece un resumen con toda la información de la configuración que ha realizado. Revise esta información y utilice el botón **Atrás** para realizar modificaciones, si es que es necesario. Una vez satisfecho, haga clic en el botón **Terminar** e inicie el proceso de instalación.



    Una ventana VNC se abre para mostrar el inicio del proceso de instalación del sistema operativo de huésped.

Así concluye el proceso general para crear huéspedes con **`virt-manager`**. El *Capítulo 5, Introducción a la instalación de un huésped virtualizado* contiene instrucciones detalladas para instalar una variedad de sistemas operativos comunes.

5.4. Instalación de huéspedes con PXE

Esta sección describe los pasos necesarios para instalar huéspedes con PXE. La instalación de huéspedes PXE requiere un dispositivo de red compartido, también conocido como un puente de red. El procedimiento que mostramos a continuación detalla la creación de un puente, y los pasos requeridos para utilizar dicho puente para un instalación PXE.

1. **Crear un nuevo puente**
   a. Cree un nuevo archivo de script de red en el directorio **`/etc/sysconfig/network-scripts/`**. Este ejemplo crea un archivo denominado **`ifcfg-installation`**, el cual crea un puente llamado *`installation`*.

```
# cd /etc/sysconfig/network-scripts/
# vim ifcfg-installation
DEVICE=installation
TYPE=Bridge
BOOTPROTO=dhcp
ONBOOT=yes
```

Advertencia

The line, *`TYPE=Bridge`*, is case-sensitive. It must have uppercase 'B' and lower case 'ridge'.

   b. Inicie el nuevo puente reiniciando el servicio de red. El comando **`ifup installation`** puede iniciar el puente individual, pero es más seguro verificar que la red en su totalidad se reinicie adecuadamente.

```
# service network restart
```

   c. No hay interfaces añadidas al nuevo puente aún. Utilice el comando **`brctl show`** para ver información sobre puentes de red en el sistema.

```
# brctl show
bridge name     bridge id               STP enabled     interfaces
installation    8000.000000000000       no
virbr0          8000.000000000000       yes
```

   El puente **`virbr0`** es un puente por defecto utilizado por **`libvirt`** para Traducción de dirección de red (NAT) en el dispositivo Ethernet predeterminado.

2. **Añada una interfaz al nuevo puente**
   Edite el archivo de configuración para la interfaz. Añada el parámetro **`BRIDGE`** al archivo de configuración con el nombre del puente creado en los pasos anteriores.

```
# Intel Corporation Gigabit Network Connection
DEVICE=eth1
BRIDGE=installation
BOOTPROTO=dhcp
HWADDR=00:13:20:F7:6E:8E
ONBOOT=yes
```

   Después de editar el archivo de configuración, reinicie la red o vuelva a arrancar.

```
# service network restart
```

Verifique que la interfaz esté conectada al comando **`brctl show`**:

```
# brctl show
bridge name     bridge id               STP enabled     interfaces
installation    8000.001320f76e8e       no              eth1
virbr0          8000.000000000000       yes
```

3. **Configuración de seguridad**
   Configure **`iptables`** para permitir que todo el tráfico sea reenviado a través del puente.

```
# iptables -I FORWARD -m physdev --physdev-is-bridged -j ACCEPT
# service iptables save
# service iptables restart
```

Deshabilite iptables sobre los puentes

De manera alternativa, evite que el tráfico puenteado sea procesado por reglas de **`iptables`**. En el archivo **`/etc/sysctl.conf`** agregue las siguientes líneas:

```
net.bridge.bridge-nf-call-ip6tables = 0
net.bridge.bridge-nf-call-iptables = 0
net.bridge.bridge-nf-call-arptables = 0
```

Vuelva a cargar los parámetros del kernel configurados con **`sysctl`**.

```
# sysctl -p /etc/sysctl.conf
```

4. **Reiniciar libvirt antes de la instalación**
   Reinicie el demonio **`libvirt`**.

```
# service libvirtd reload
```

El puente está configurado, ahora puede comenzar la instalación.

Instalación PXE con virt-install

Para **`virt-install`** añada el parámetro de instalación **`--network=bridge:installation`** donde *`installation`* es el nombre de su puente. Para instalaciones PXE utilice el parámetro `--pxe`.

```
# virt-install --accelerate --hvm --connect qemu:///system \
    --network=bridge:installation --pxe\
    --name EL10 --ram=756 \
    --vcpus=4
    --os-type=linux --os-variant=rhel5
    --file=/var/lib/libvirt/images/EL10.img \
```

Ejemplo 5.3. Instalación PXE con virt-install

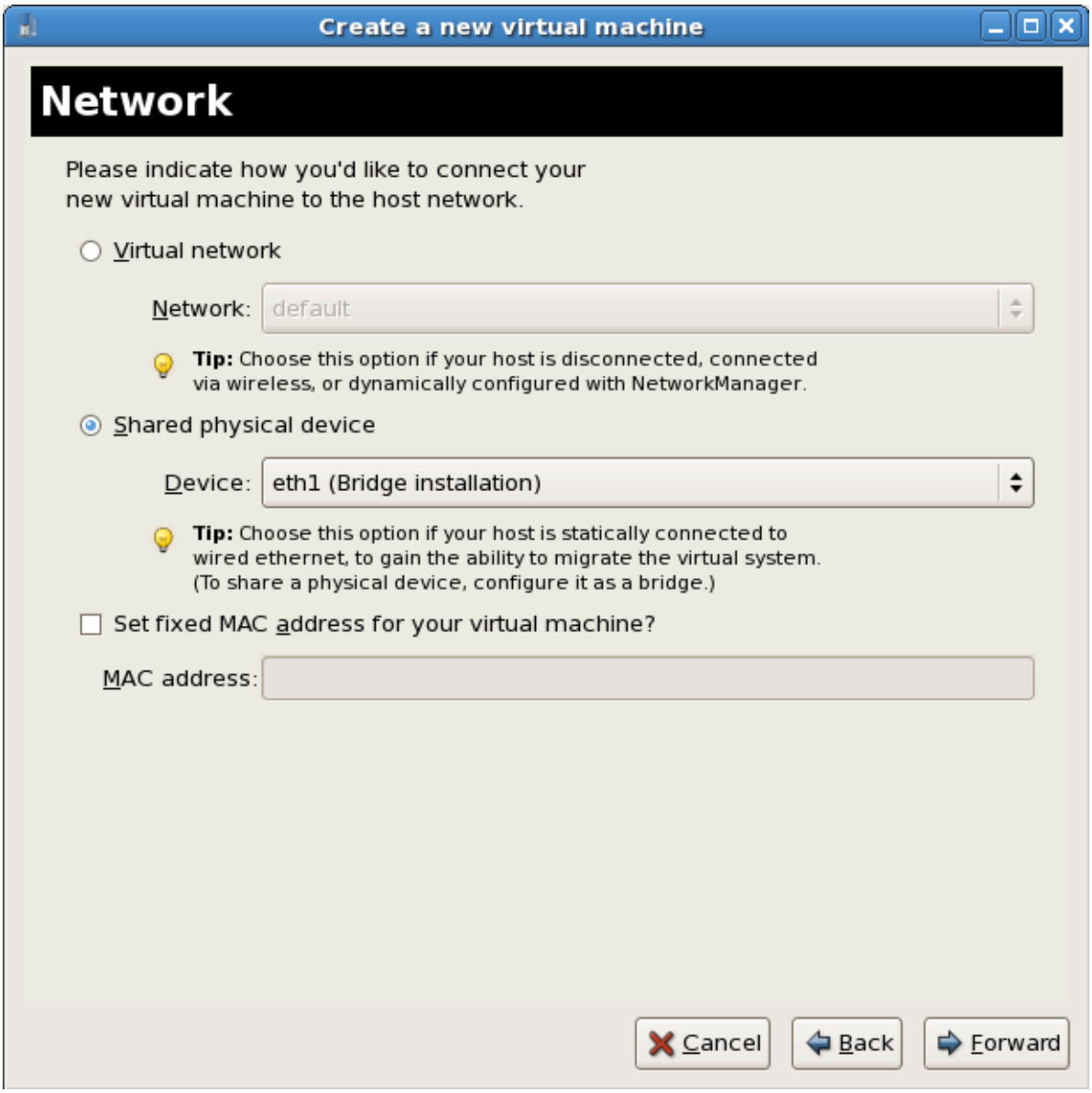
Instalación PXE con virt-manager

Los pasos que mostramos a continuación son aquellos que difieren de los procedimientos estándares de instalación de **`virt-manager`**.

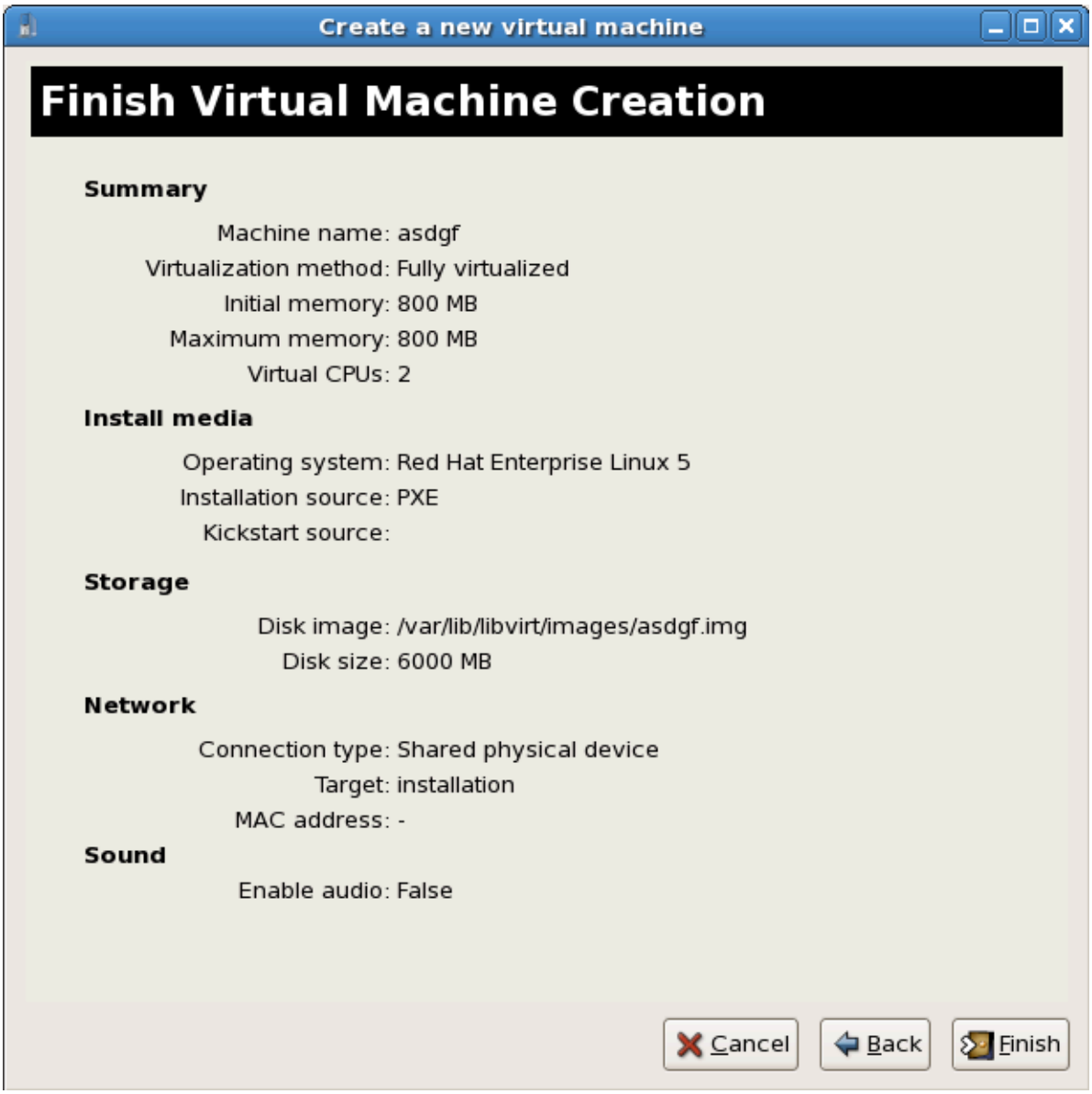
1. **Seleccionar PXE**
   Seleccionar PXE como el medio de instalación

Create a new virtual machine
Installation Method
Please indicate where installation media is available for the operating system you would like to install on this virtual machine:
Local install media (ISO image or CDROM)
Network install tree (HTTP, FTP, or NFS)
Network boot (PXE)
Please choose the operating system you will be installing on the virtual machine:
OS Type: Linux
OS Variant: Red Hat Enterprise Linux 5
Not all operating system choices are supported by Red Hat. Please see the link below for supported configurations:
Red Hat Enterprise Linux 5 virtualization support
Cancel
Back
Forward

2. **Seleccionar el puente**
   Seleccione **Dispositivo físico compartido** y elija el puente creado en el procedimiento anterior.


Create a new virtual machine
Network
Please indicate how you'd like to connect your new virtual machine to the host network.
Virtual network
Network:
default
Tip: Choose this option if your host is disconnected, connected via wireless, or dynamically configured with NetworkManager.
Shared physical device
Device:
eth1 (Bridge installation)
Tip: Choose this option if your host is statically connected to wired ethernet, to gain the ability to migrate the virtual system. (To share a physical device, configure it as a bridge.)
Set fixed MAC address for your virtual machine?
MAC address:
Cancel
Back
Forward

3. **Iniciar la instalación**
   La instalación está lista para empezar.



Una solicitud de DHCP es enviada y si se encuentra un servidor válido PXE, los procesos de instalación de huésped iniciarán.

Cómo instalar Linux para empresas de Red Hat 5 como un huésped completamente virtualizado

Esta sección detalla la instalación en un equipo de Fedora de un huésped Linux para Empresas de Red Hat 5 completamente virtualizado.

Procedimiento 6.1. Creación de un huésped completamente virtualizado de Red Hat Enterprise Linux 5 con virt-manager

1. **Abrir virt-manager**
   Inicie **`virt-manager`**: Abra la aplicación **Administrador de máquina virtual** desde el menú **Aplicaciones**, **Herramientas del sistema**. De manera alternativa, ejecute el comadno **`virt-manager`** como usuario root.

2. **Seleccione el hipervisor**
   Seleccione el hipervisor. Tenga en cuenta que actualmente al hipersvisor de KVM se lo denomina **`qemu`**.

   Si aún no lo ha hecho, conéctese a un hipervisor. Abra el menú **Archivo** y elija la opción **Añadir conexión...**. Consulte la *Sección 29.1, “La ventana de agregado de conexión”*.

   Una vez haya seleccionado la conexión del hipervisor el botón **Nueva** aparece. Presione el botón **Nueva**.

3. **Inicie el asistente para nueva máquina virtual**
   Al presionar el botón **Nuevo** se inicia el asistente para la creación de máquinas virtuales.

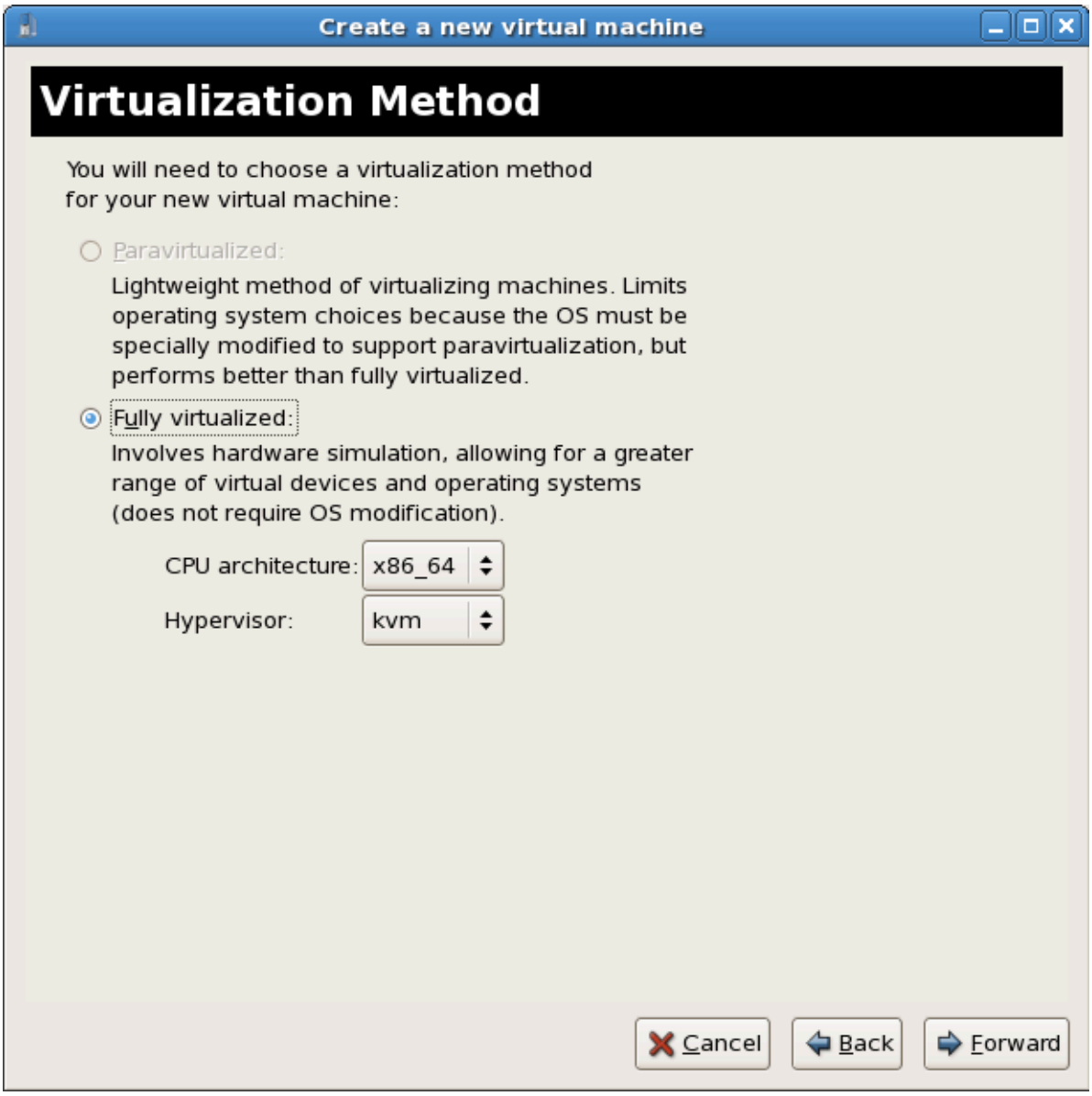
Create a new virtual machine
Virtual Machine Creation
This assistant will guide you through creating a new virtual machine. You will be asked for some information about the virtual machine you'd like to create, such as:
A name for your new virtual machine
Whether the virtual machine will be fully virtualized or para-virtualized
The location of the files necessary for installing an operating system on the virtual machine
Storage details - which disk partitions or files the virtual machine should use
Memory and CPU allocation
Cancel
Back
Forward

Presione **Adelante** para continuar.

4. **Identifique con un nombre a la máquina virtual**
   Provide a name for your virtualized guest. The following punctuation and whitespace characters are permitted for '_', '**.**' and '**-**' characters.

Press **Forward** to continue.

5. **Elija un método de virtualización**
   Elija el método de virtualización para el huésped virtualizado. Tenga en cuenta que sólo puede elegir entre x86_64 (64 bits) and x86 (32 bits).


Create a new virtual machine
Virtualization Method
You will need to choose a virtualization method for your new virtual machine:
Paravirtualized:
Lightweight method of virtualizing machines. Limits operating system choices because the OS must be specially modified to support paravirtualization, but performs better than fully virtualized.
Fully virtualized:
Involves hardware simulation, allowing for a greater range of virtual devices and operating systems (does not require OS modification).
CPU architecture: x86_64
Hypervisor: kvm
Cancel
Back
Forward

Haga clic en **Adelante** para continuar.

6. **Seleccione el método de instalación**
   Linux para empresas de Red Hat puede instalarse utilizando alguno de los siguientes métodos:

   - **medio de instalación local**, o bien una imagen ISO, o bien un medio físico óptico.
   - Seleccione **Arbol de instalación de red** si tiene alojado en algún lado de su red (mediante HTTP, FTP o NFS) el árbol de instalación de Linux para empresas de Red Hat.
   - Puede utilizarse PXE si usted tiene un servidor PXE configurado para arrancar un medio de instalación de Linux para empresas de Red Hat. Esta configuración no se desarolla en esta guía. Sin embargo, la mayoría de los pasos para realizar esta instalación son los mismos una vez que el medio es iniciado.

   Establezca el **Tipo de SO** a **Linux** y **Variante de SO** a **Linux para Empresas de Red Hat 5**, tal como se muestra en el pantallazo.

Create a new virtual machine
Installation Method
Please indicate where installation media is available for the operating system you would like to install on this virtual machine:
Local install media (ISO image or CDROM)
Network install tree (HTTP, FTP, or NFS)
Network boot (PXE)
Please choose the operating system you will be installing on the virtual machine:
OS Type: Linux
OS Variant: Red Hat Enterprise Linux 5
Not all operating system choices are supported by Red Hat. Please see the link below for supported configurations:
Red Hat Enterprise Linux 5 virtualization support
Cancel
Back
Forward

Presione **Siguiente** para continuar.

7. **Ubique el medio de instalación**
   Seleccione la ubicación de la imagen ISO o el dispositivo de CD-ROM o DVD. Este ejemplo utiliza un archivo de imagen ISO de la instalación de DVD de Linux para Empresas de Red Hat.

   a. Haga clic en el botón **Browse**.

   b. Busque la ubicación del archivo ISO y selecciones la imagen ISO. Presione **Abrir** para confirmar su elección.

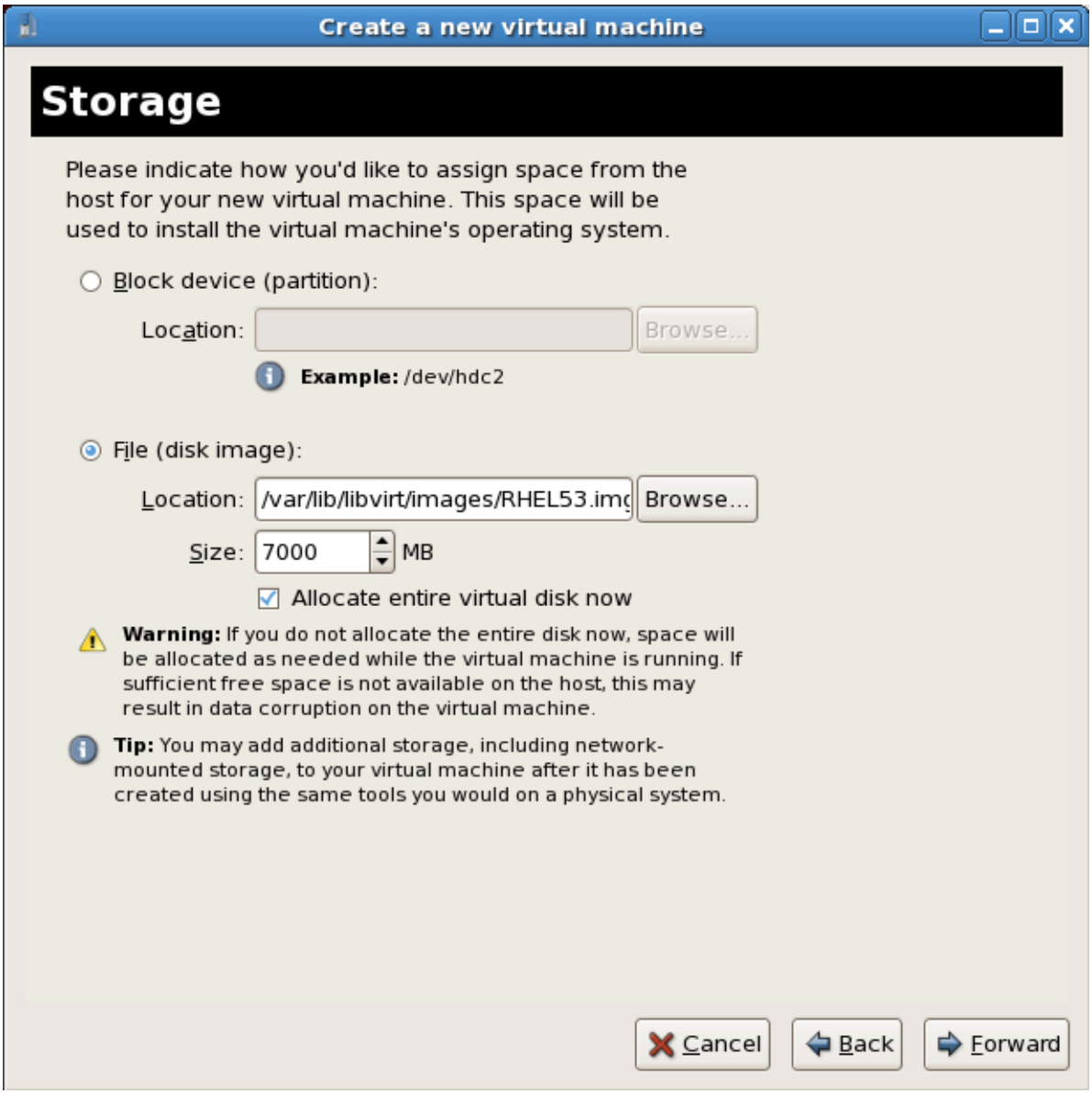
   c. El archivo es seleccionado y queda listo para ser instalado.

Presione **Adelante** para continuar.

SELinux y los archivos de imagen

Para archivos de imagen ISO, e imágenes de almacenamiento de huéspedes, se recomienda utilizar el directorio **`/var/lib/libvirt/images/`**. Cualquier otra ubicación puede necesitar una configuración adicional de SELinux, consulte los detalles en *Sección 19.2, "SELinux y virtualización completas"*.

8. **Configuración del almacenamiento**
   Asigne un dispositivo de almacenamiento físico (**Dispositivos de bloque**) o una imagen de archivo (**Archivo**). Las imágenes basadas en archivo deben ser almacenadas en el directorio **`/var/lib/libvirt/images/`**. Asigne espacio suficiente para su huésped virtualizado y para cualquier aplicación que requiera


Create a new virtual machine
Storage
Please indicate how you'd like to assign space from the host for your new virtual machine. This space will be used to install the virtual machine's operating system.
Block device (partition):
Location:
Browse...
Example: /dev/hdc2
File (disk image):
Location: /var/lib/libvirt/images/RHEL53.img
Browse...
Size: 7000 MB
Allocate entire virtual disk now
Warning: If you do not allocate the entire disk now, space will be allocated as needed while the virtual machine is running. If sufficient free space is not available on the host, this may result in data corruption on the virtual machine.
Tip: You may add additional storage, including network-mounted storage, to your virtual machine after it has been created using the same tools you would on a physical system.
Cancel
Back
Forward

Presione**Adelante** para continuar.

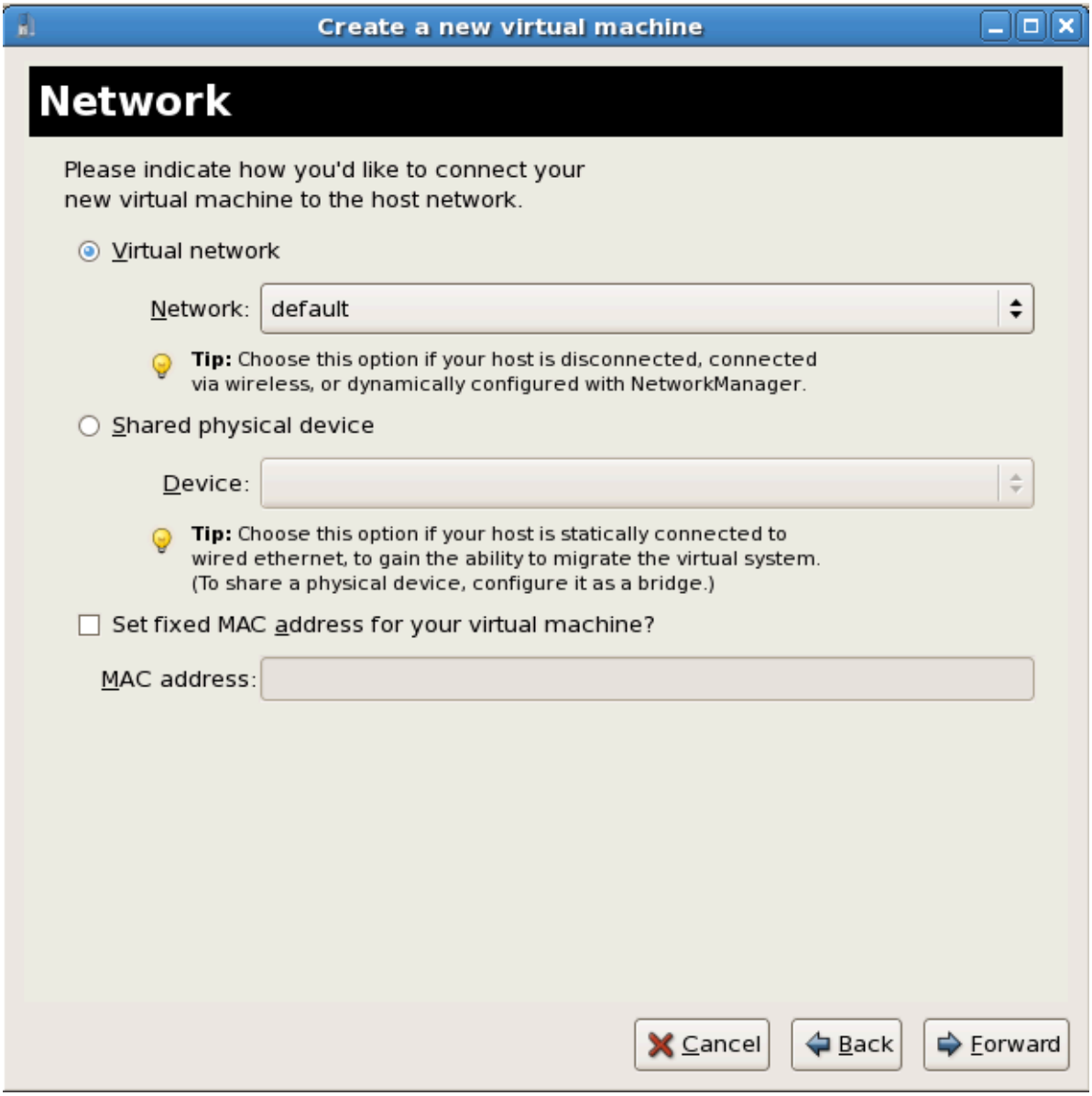
Migración

Las migraciones en vivo y desconectadas requieren que los huéspedes sean instalados en un almacenamiento de red compartido. Para obtener información sobre la configuración de almacenamiento compartido para huéspedes, consulte el *Parte V, “Cuestiones relacionadas con el almacenamiento en virtualización”*.

9. **Configuración de la red**
   Seleccione o bien **Red virtual**, o bien **Dispositivo físico compartido**.

   La opción de red virtual utiliza el protocolo de Traducción de dirección de red (NAT, por las iniciales en inglés de Network Address Translation) para compartir el dispositivo de red predeterminado con el huésped virtualizado. Utilice la opción de red virtual para redes inalámbricas.

La opción de sispositivo físico compartido utiliza un enlace de red para darle al huésped virtualizado un acceso total al dispositivo de red.

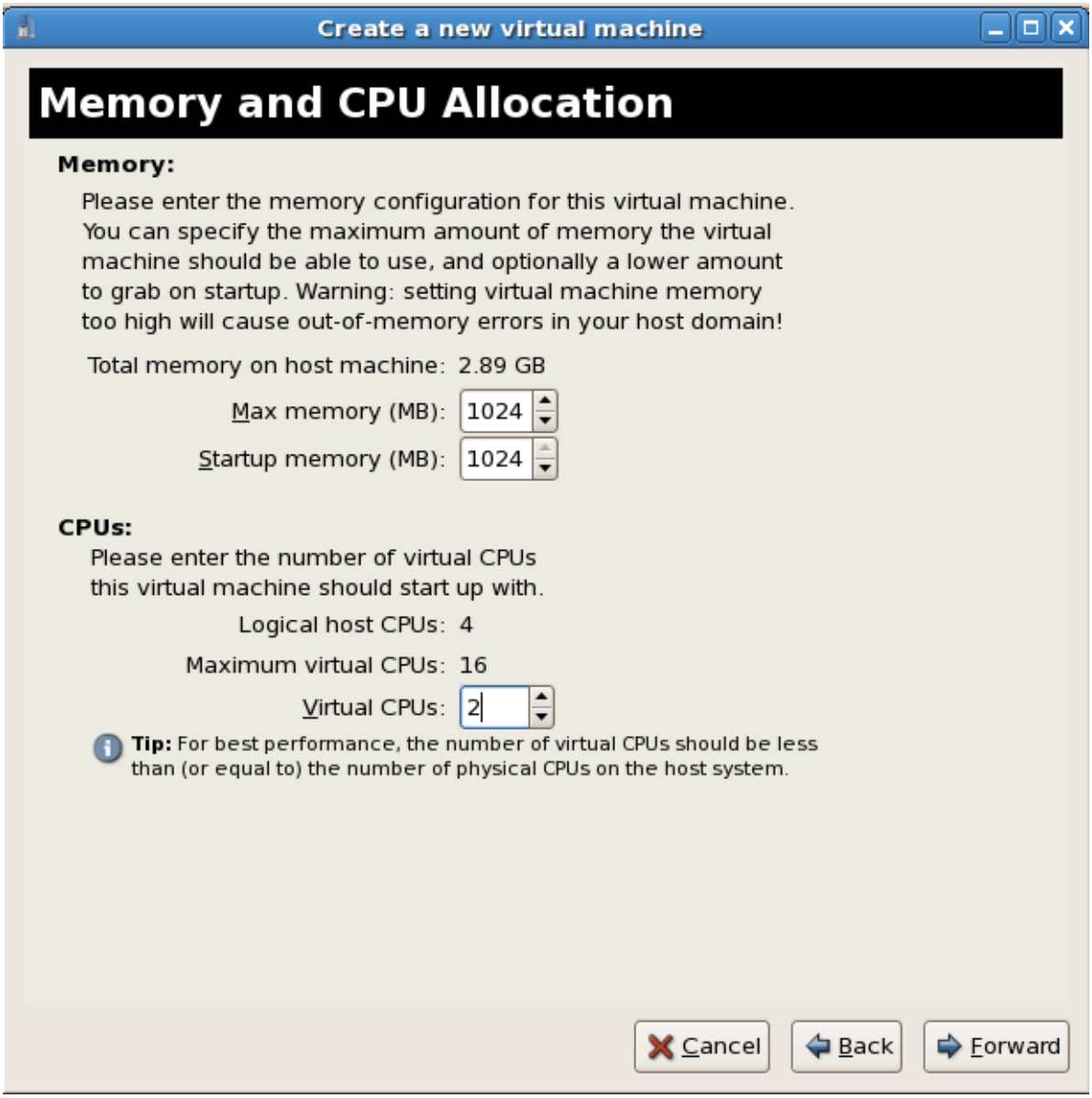

Create a new virtual machine
Network
Please indicate how you'd like to connect your new virtual machine to the host network.
Virtual network
Network: default
Tip: Choose this option if your host is disconnected, connected via wireless, or dynamically configured with NetworkManager.
Shared physical device
Device:
Tip: Choose this option if your host is statically connected to wired ethernet, to gain the ability to migrate the virtual system. (To share a physical device, configure it as a bridge.)
Set fixed MAC address for your virtual machine?
MAC address:
Cancel
Back
Forward

Presione **Adelante** para continuar.

10. **Alojamiento del CPU y de la memoria**
    The **Memory and CPU Allocation** window displays. Choose appropriate values for the virtualized CPUs and RAM allocation. These values affect the host's and guest's performance.

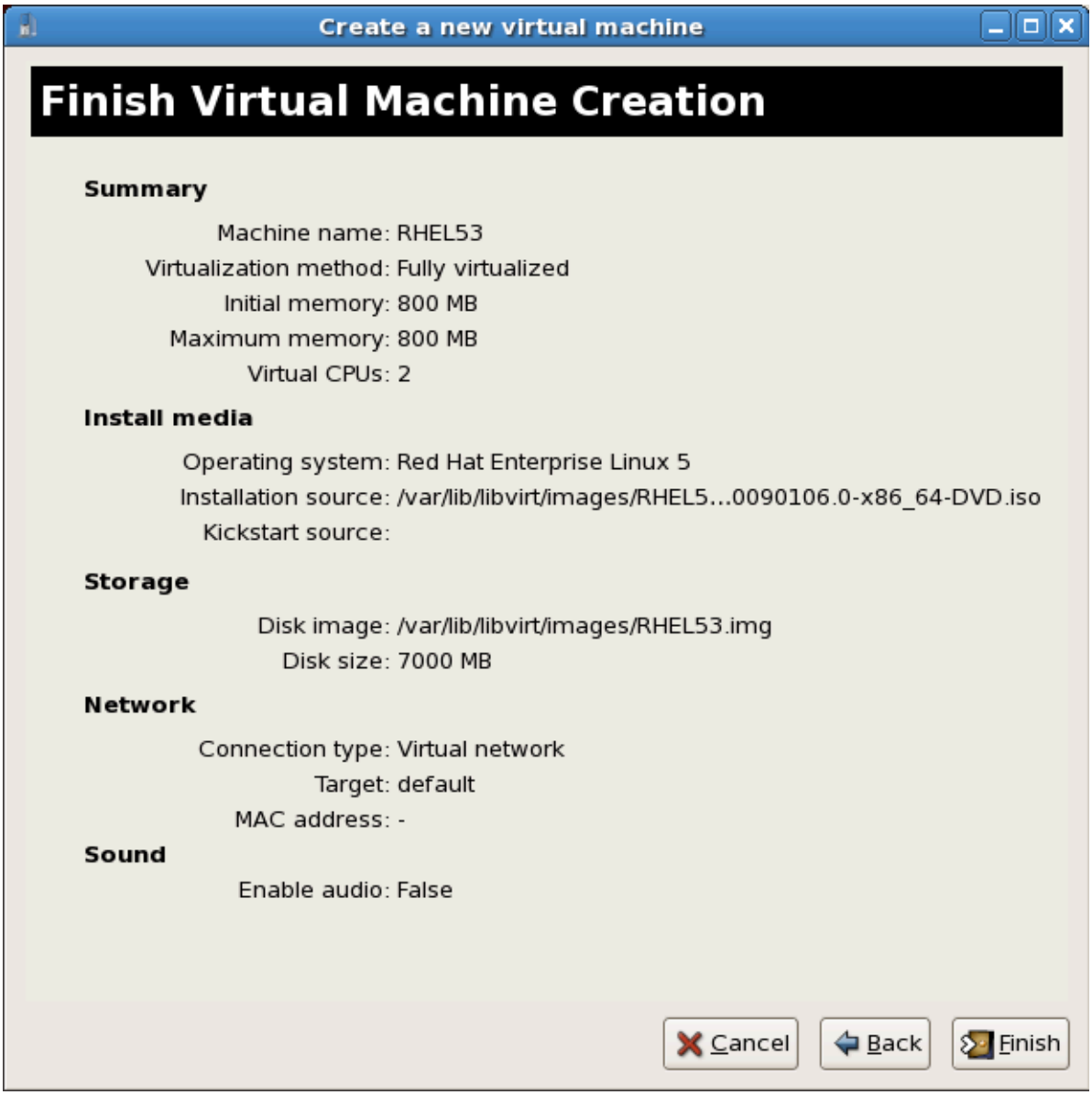
    Los huéspedes virtualizados requieren de suficiente memoria física (RAM) para ejecutarse eficiente y eficazmente. Elija una valor de memoria apto para los requerimientos de su sistema operativo huésped, y para sus aplicaciones. Recuerde que los huéspedes utilizan RAM física. La ejecución de demasiados huéspedes, o destinar un resto de memoria insuficiente para el sistema del equipo anfitrión, causará una utilización significativa de la memoria virtual y del espacio de intercambio. La memoria virtual es notoriamente más lenta, y esto hace que el rendimiento y receptividad del sistema se degrade. Asegúrese de asignar suficiente memoria para que todos los huéspedes y el equipo anfitrión operen de modo eficaz.

Asigne suficientes CPUs virtuales para el huésped virtualizado. Si el huésped ejecuta una aplicación múltiple, asigne la cantidad de CPUs virtuales necesarias para que el huésped se ejecute de manera apropiada. No asigne mayor cantidad de CPUs virtuales, que la de procesadores físicos disponibles en el equipo anfitrión. Si bien es posible sobrealojar procesadores virtuales, el sobrealojamiento tiene un efecto significativo y negativo sobre el desempeño tanto del equipo como de los huéspedes. Esto es debido al contexto de intercambio de procesos generales del procesador.


Create a new virtual machine
Memory and CPU Allocation
Memory:
Please enter the memory configuration for this virtual machine. You can specify the maximum amount of memory the virtual machine should be able to use, and optionally a lower amount to grab on startup. Warning: setting virtual machine memory too high will cause out-of-memory errors in your host domain!
Total memory on host machine: 2.89 GB
Max memory (MB): 1024
Startup memory (MB): 1024
CPUs:
Please enter the number of virtual CPUs this virtual machine should start up with.
Logical host CPUs: 4
Maximum virtual CPUs: 16
Virtual CPUs: 2
Tip: For best performance, the number of virtual CPUs should be less than (or equal to) the number of physical CPUs on the host system.
Cancel
Back
Forward

Presione **Adelante** para continuar.

11. **Verifique las configuraciones, e inicie la instalación del huésped**
Verifique la configuración.



Presione **Terminar** para iniciar el procedimiento de instalación de huésped.

12. **Cómo instalar Linux para empresas de Red Hat**
    Complete la secuencia de instalación del Linux para Empresas de Red Hat. La secuencia de instalación se describe en la *Guía de Instalación*, disponible en *Red Hat Documentation*[1].

Está listo para instalarse un un huésped completamente virtualizado de Linux para empresas de Red Hat 5.

Instalación de Windows XP como huésped completamente virtualizado

Windows XP puede ser instalado como un huésped completamente virtualizado. Esta sección describe cómo hacerlo.

Antes de comenzar este procedimiento asegúrese de tener acceso de root.

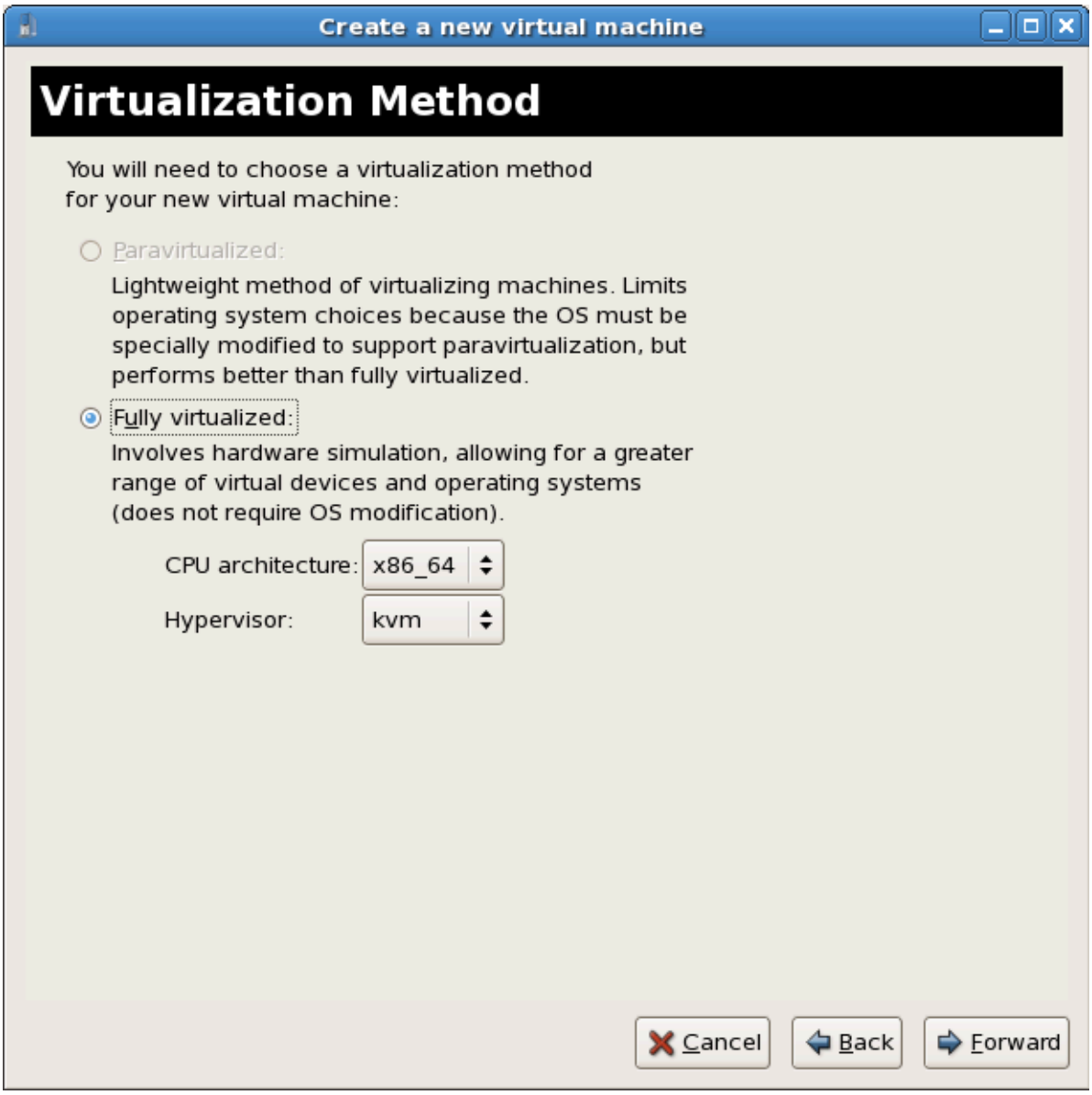
1. **Cómo iniciar virt-manager**

   Open **Applications > System Tools > Virtual Machine Manager**. Open a connection to a host (click **File > Add Connection**). Click the **New** button to create a new virtual machine.

2. **Cómo denonimar a su huésped**
   Ingrese el **Nombre de sistema** y haga clic en el botón **Adelante**.

3. **Elección de un método de virtualización**
   Aparece la ventana de **Elegir un método de virtualización**.

   Una virtualización completa necesita un procesador con las extensiones AMD 64 y AMD-V, o un procesador con las extensiones Intel 64 e Intel VT. Si estas extensiones no se encuentran presentes, KVM no estará disponible.


Create a new virtual machine
Virtualization Method
You will need to choose a virtualization method for your new virtual machine:
Paravirtualized:
Lightweight method of virtualizing machines. Limits operating system choices because the OS must be specially modified to support paravirtualization, but performs better than fully virtualized.
Fully virtualized:
Involves hardware simulation, allowing for a greater range of virtual devices and operating systems (does not require OS modification).
CPU architecture: x86_64
Hypervisor: kvm
Cancel
Back
Forward

   Haga clic en **Avanzar** para continuar.

4. **Elección de un método de instalación**
   Esta pantalla le permite especificar el método de instalación y el tipo de sistema operativo.

   Seleccione **Windows** desde la lista de **Tipo de sistema operativo** y **Microsoft Windows XP** desde la lista de **Variante de sistema operativo**.

   La instalación PXE no se cubre en este capítulo.

Create a new virtual machine
Installation Method
Please indicate where installation media is available for the operating system you would like to install on this virtual machine:
Local install media (ISO image or CDROM)
Network install tree (HTTP, FTP, or NFS)
Network boot (PXE)
Please choose the operating system you will be installing on the virtual machine:
OS Type: Windows
OS Variant: Microsoft Windows XP (x86)
Not all operating system choices are supported by Red Hat. Please see the link below for supported configurations:
Red Hat Enterprise Linux 5 virtualization support
Cancel
Back
Forward

Archivos de imágenes y SELinux

Para archivos de imagen ISO e imágenes de almacenamiento, se recomienda utilizar el directorio **`/var/lib/libvirt/images/`**. Cualquier otra ubicación puede requerir una configuración adicional de SELinux. Para obtener mayor información, consulte *Sección 19.2, "SELinux y virtualización completas"*.

Haga clic en **Avanzar** para continuar.

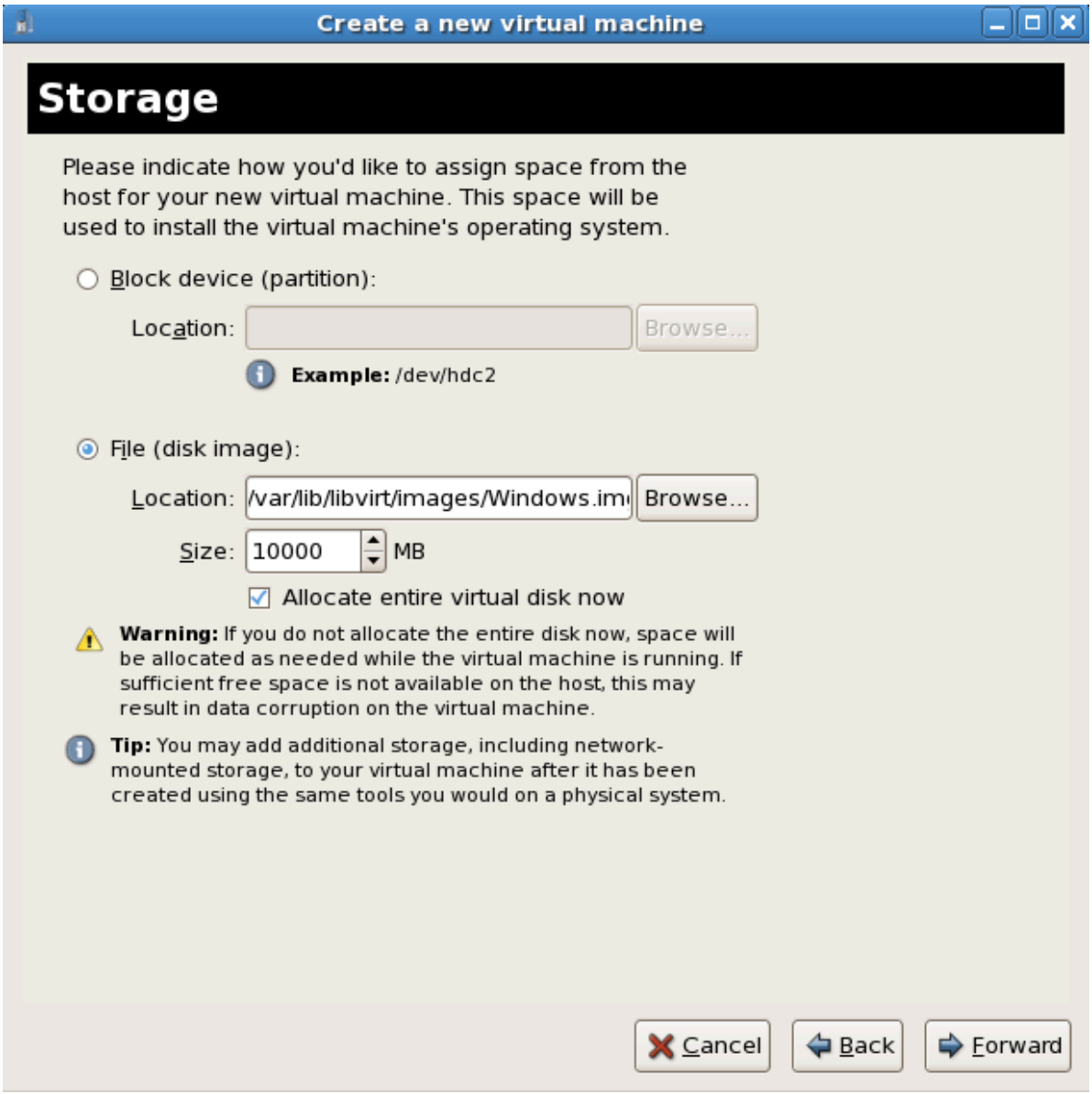
5. **Elección de una imagen de instalación**
   Elija la imagen de instalación, o el CD-ROM. Para instalaciones de CD-ROM o DVD, seleccione el dispositivo que contenga el disco de instalación de Windows. Si escoge **Ubicación de imagen ISO**, ingrese la ruta para la instalación de la imagen .iso de Windows.

Haga clic en **Avanzar** para continuar.

6. The **Storage** window displays. Choose a disk partition, LUN or create a file-based image for the guest's storage.

   Todos los archivos de imagen deberían ser almacenados en el directorio **`/var/lib/libvirt/images/`**. Cualquier otra ubicación de imágenes basadas en archivo están prohibidas por SELinux. Si usted ejecuta SELinux en modo obediente, consulte *Sección 19.2, "SELinux y virtualización completas"* para obtener mayor información sobre la instalación de huéspedes.

   Aloje espacio adicional en caso de que el huésped lo necesite para aplicaciones u otros datos. Por ejemplo, los servidores web necesitan espacio adicional para los archivos de registro.


Create a new virtual machine
Storage
Please indicate how you'd like to assign space from the host for your new virtual machine. This space will be used to install the virtual machine's operating system.
Block device (partition):
Location:
Browse...
Example: /dev/hdc2
File (disk image):
Location: /var/lib/libvirt/images/Windows.im
Browse...
Size: 10000 MB
Allocate entire virtual disk now
Warning: If you do not allocate the entire disk now, space will be allocated as needed while the virtual machine is running. If sufficient free space is not available on the host, this may result in data corruption on the virtual machine.
Tip: You may add additional storage, including network-mounted storage, to your virtual machine after it has been created using the same tools you would on a physical system.
Cancel
Back
Forward

Elija el tamaño adecuado de su huésped en el tipo de almacenamiento que haya seleccionado, y haga clic en el botón **Avanzar**.

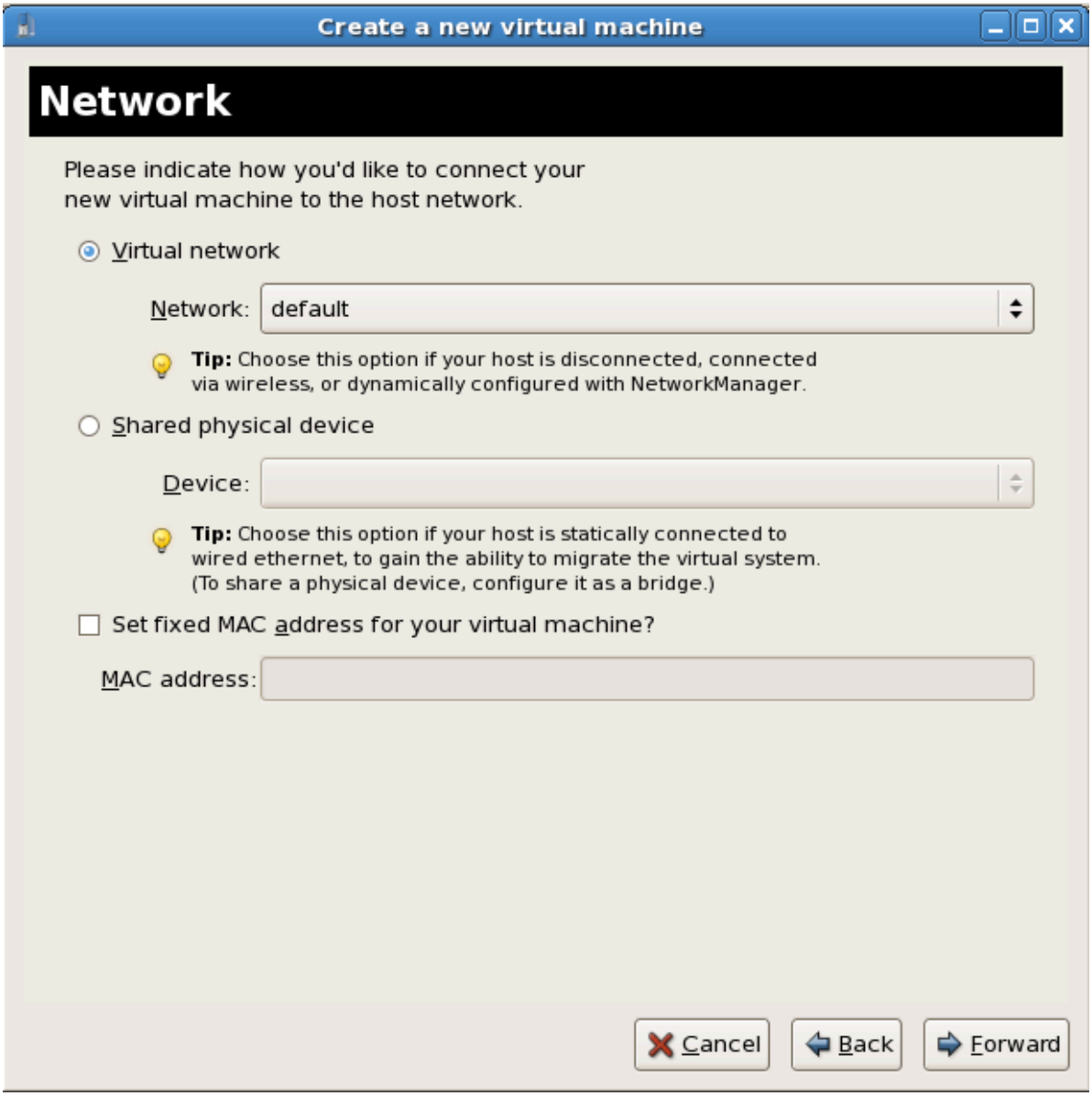
Nota

Se recomienda utilizar el directorio predeterminado para imágenes de máquina virtual, **`/var/lib/libvirt/images/`**. Si está utilizando una ubicación diferente (tal como **`/images/`** en este ejemplo),asegúrese de que haya añadido su política de SELinux y de volverla a etiquetar antes de continuar con la instalación (más adelante en el documento encontrará información sobre cómo modificar su política de SELinux)

7. **Configuración de la red**
   Elija o bien **Red virtual**, o bien **Dispositivo físico compartido**.

La opción de red virtual utiliza el protocolo de Traducción de direcciones de red (NAT, por las iniciales en inglés de Network Address Translation) para compartir el dispositivo de red predeterminado con el huésped virtualizado. Utilice la opción de red virtual para redes inalámbricas.

La opción de dispositivo físico compartido utiliza un vínculo de red que permite otorgarle total acceso al huésped virtualizado al dispositivo de red.


Create a new virtual machine
Network
Please indicate how you'd like to connect your new virtual machine to the host network.
Virtual network
Network: default
Tip: Choose this option if your host is disconnected, connected via wireless, or dynamically configured with NetworkManager.
Shared physical device
Device:
Tip: Choose this option if your host is statically connected to wired ethernet, to gain the ability to migrate the virtual system. (To share a physical device, configure it as a bridge.)
Set fixed MAC address for your virtual machine?
MAC address:
Cancel
Back
Forward

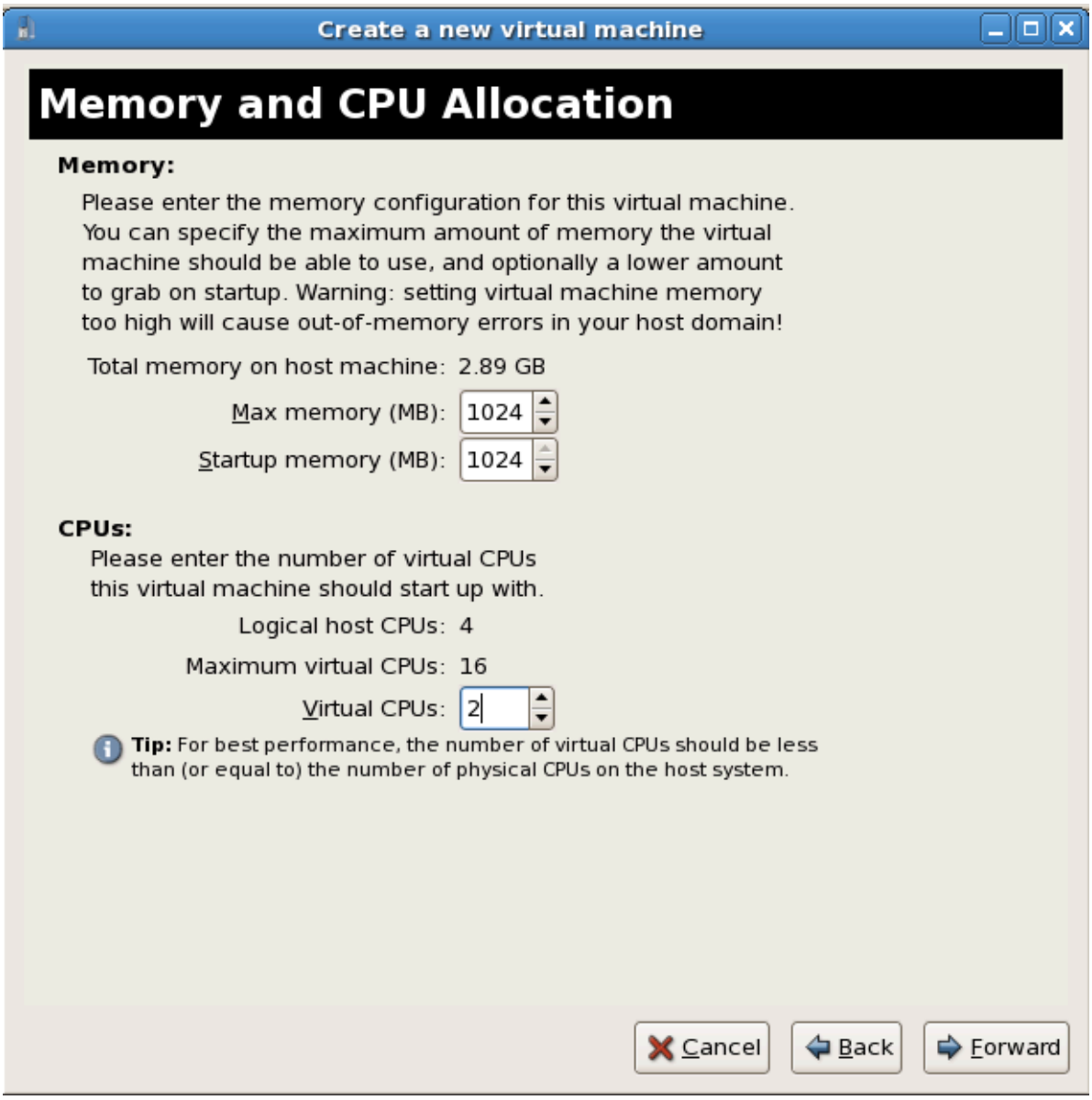
Presione **Avanzar** para continuar.

8. The **Memory and CPU Allocation** window displays. Choose appropriate values for the virtualized CPUs and RAM allocation. These values affect the host's and guest's performance.

   Los huéspedes virtualizados requieren suficiente memoria física (RAM) para ejecutar eficiente y eficazmente. Elija una valor de memoria apto para los requerimientos de su sistema operativo de huésped y aplicaciones. La mayoría de los sistemas operativos requieren al menos 512MB de RAM para funcionar con alternación. Recuerde que los huéspedes usan RAM física. La ejecución

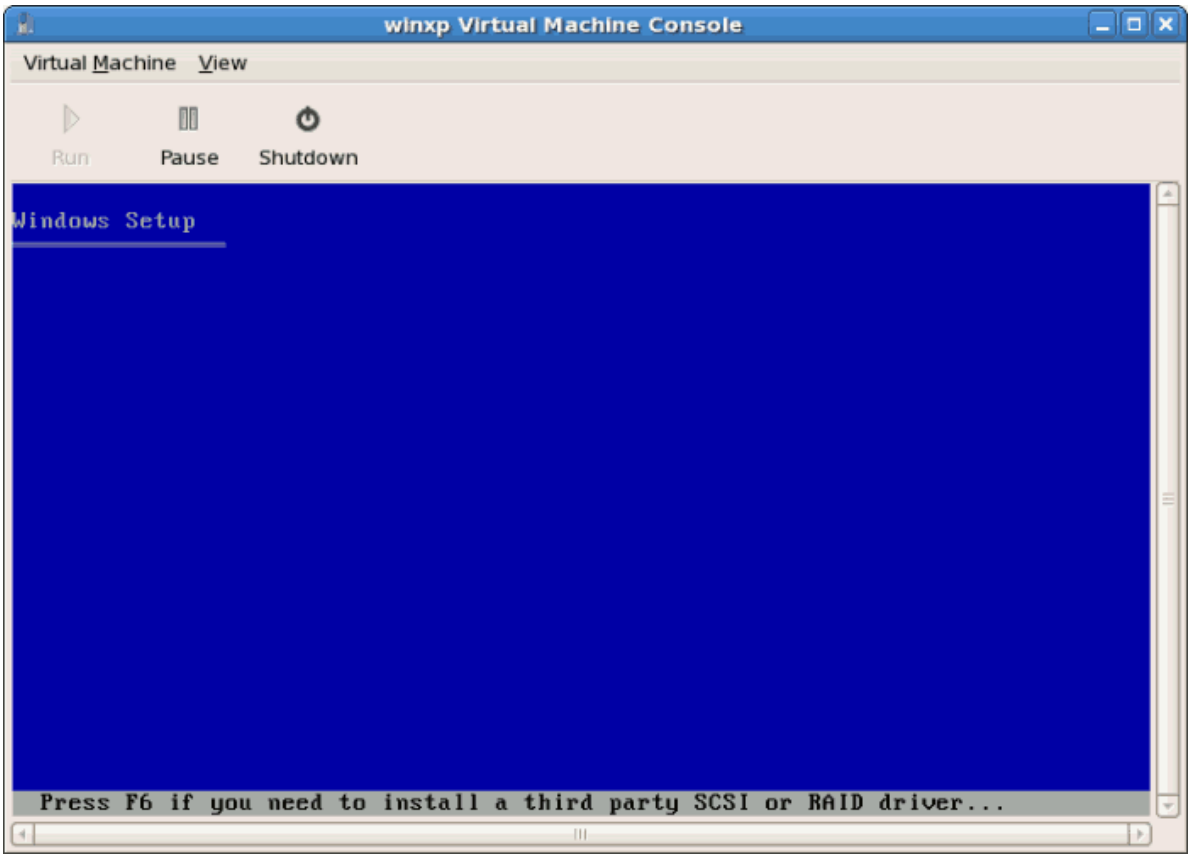
de demasiados huéspedes o dejar memoria insuficiente para el sistema de host resulta en un uso significativo de memoria virtual y de intercambio. La memoria virtual es bastante lenta lo que hace que el rendimiento y receptividad del sistema se degrade. Asegúrese de asignar suficiente memoria para que todos los huéspedes y el host operen de modo eficaz.

Asigne suficientes CPUs virtuales para el huésped virtualizado. Si el huésped ejecuta una aplicación múltiple, asigne la cantidad de CPUs virtuales necesarias para que el huésped se ejecute de manera apropiada. No asigne mayor cantidad de CPUs virtuales, que la de los procesadores físicos que se encuentren disponibles en el equipo anfitrión. Si bien es posible sobrealojar procesadores virtuales, el sobrealojamiento tiene un efecto significativo y negativo sobre el desempeño tanto del equipo como de los huéspedes. Esto es debido al contexto de intercambio de procesos generales del procesador.

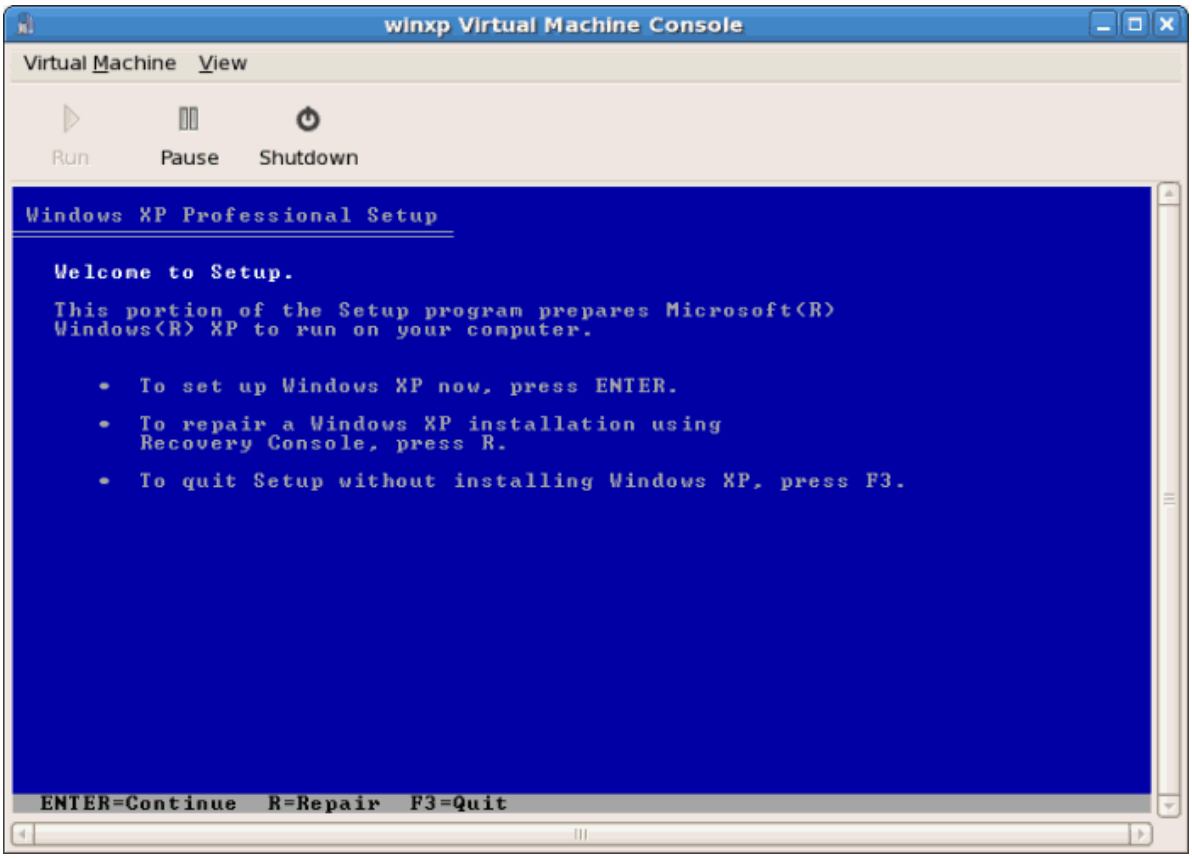

Create a new virtual machine
Memory and CPU Allocation
Memory:
Please enter the memory configuration for this virtual machine. You can specify the maximum amount of memory the virtual machine should be able to use, and optionally a lower amount to grab on startup. Warning: setting virtual machine memory too high will cause out-of-memory errors in your host domain!
Total memory on host machine: 2.89 GB
Max memory (MB): 1024
Startup memory (MB): 1024
CPUs:
Please enter the number of virtual CPUs this virtual machine should start up with.
Logical host CPUs: 4
Maximum virtual CPUs: 16
Virtual CPUs: 2
Tip: For best performance, the number of virtual CPUs should be less than (or equal to) the number of physical CPUs on the host system.
Cancel
Back
Forward

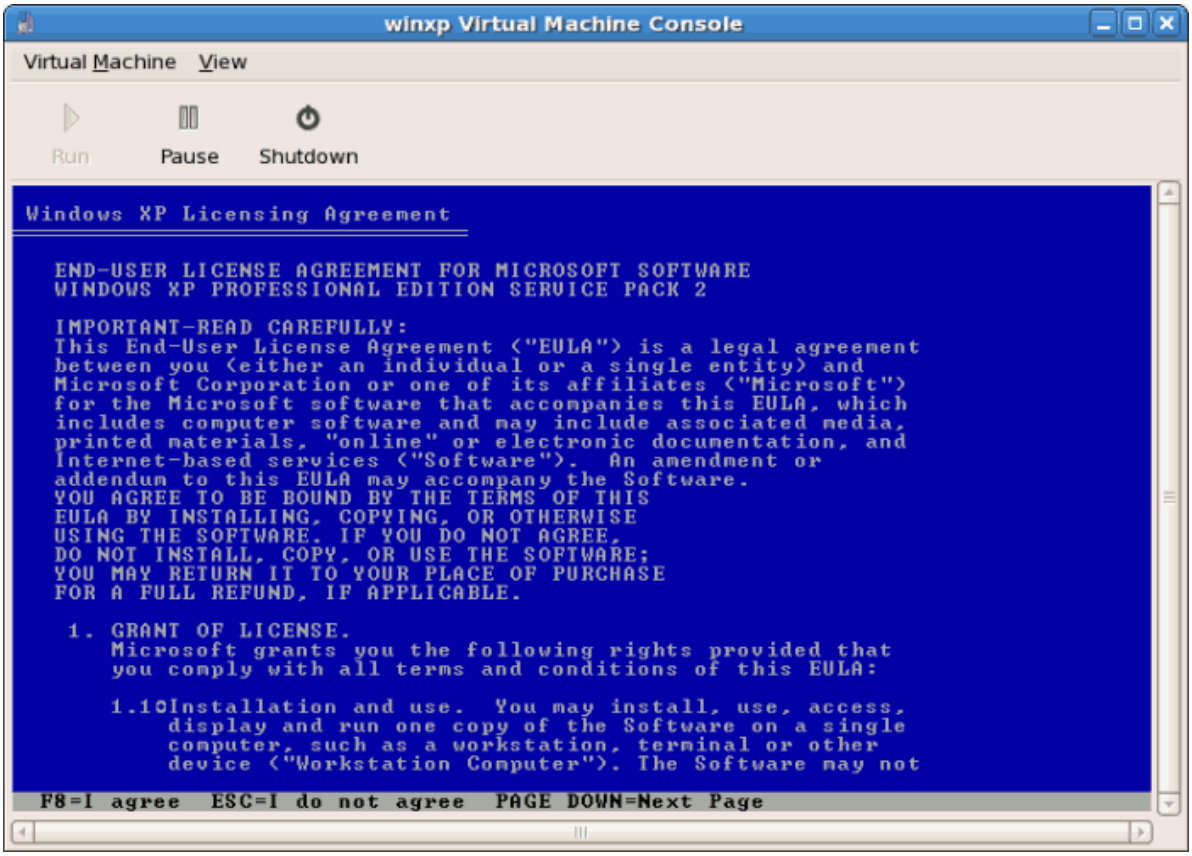
9. Antes de que la instalación continúe, aparecerá la pantalla de resumen. Presione **Terminar** para proseguir con la instalación de huésped:

10. You must make a hardware selection so open a console window quickly after the installation starts. Click **Finish** then switch to the **virt-manager** summary window and select your newly started Windows guest. Double click on the system name and the console window opens. Quickly and repeatedly press **F5** to select a new HAL, once you get the dialog box in the Windows install select the '`Generic i486 Platform`' tab. Scroll through selections with the **Up** and **Down** arrows.

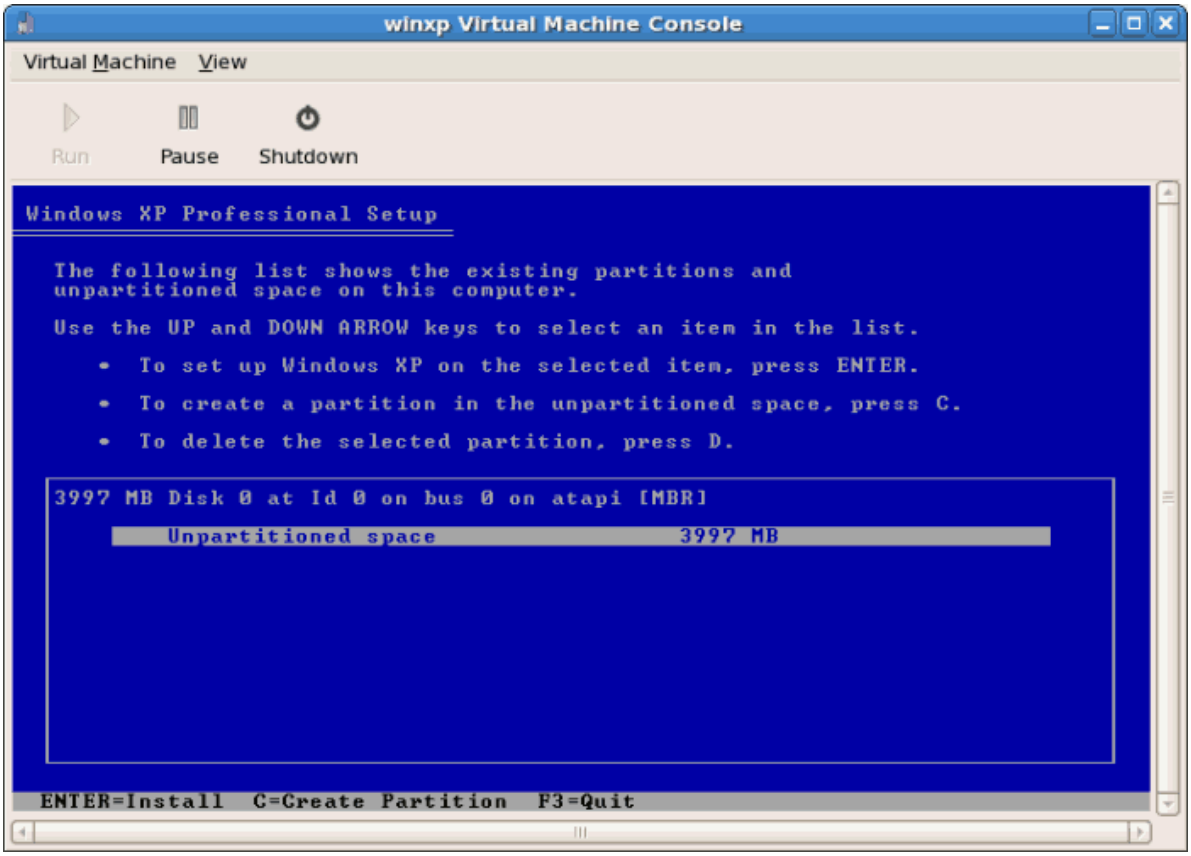


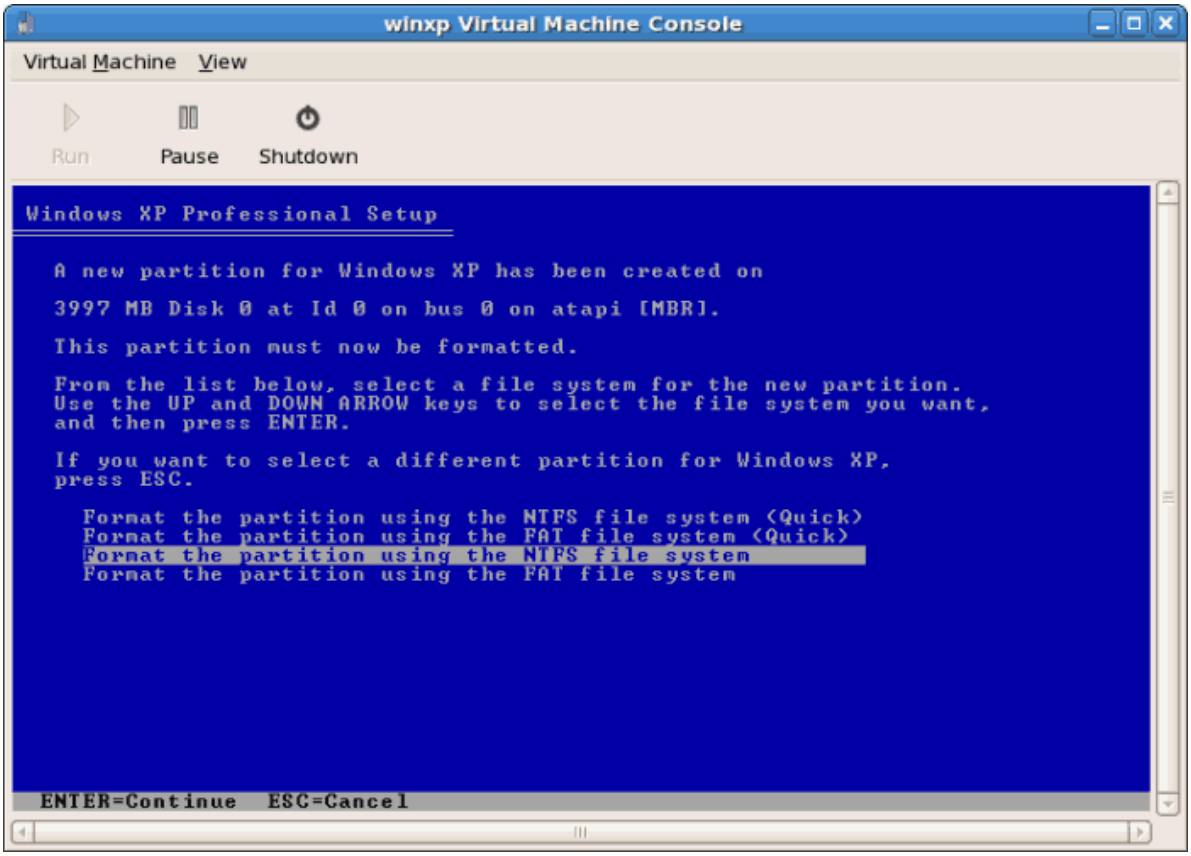
11. La instalación continúa con la instalación de Windows.


winxp Virtual Machine Console
Virtual Machine View
Run
Pause
Shutdown
Windows XP Professional Setup
Welcome to Setup.
This portion of the Setup program prepares Microsoft(R)
Windows(R) XP to run on your computer.
• To set up Windows XP now, press ENTER.
• To repair a Windows XP installation using
Recovery Console, press R.
• To quit Setup without installing Windows XP, press F3.
ENTER=Continue R=Repair F3=Quit

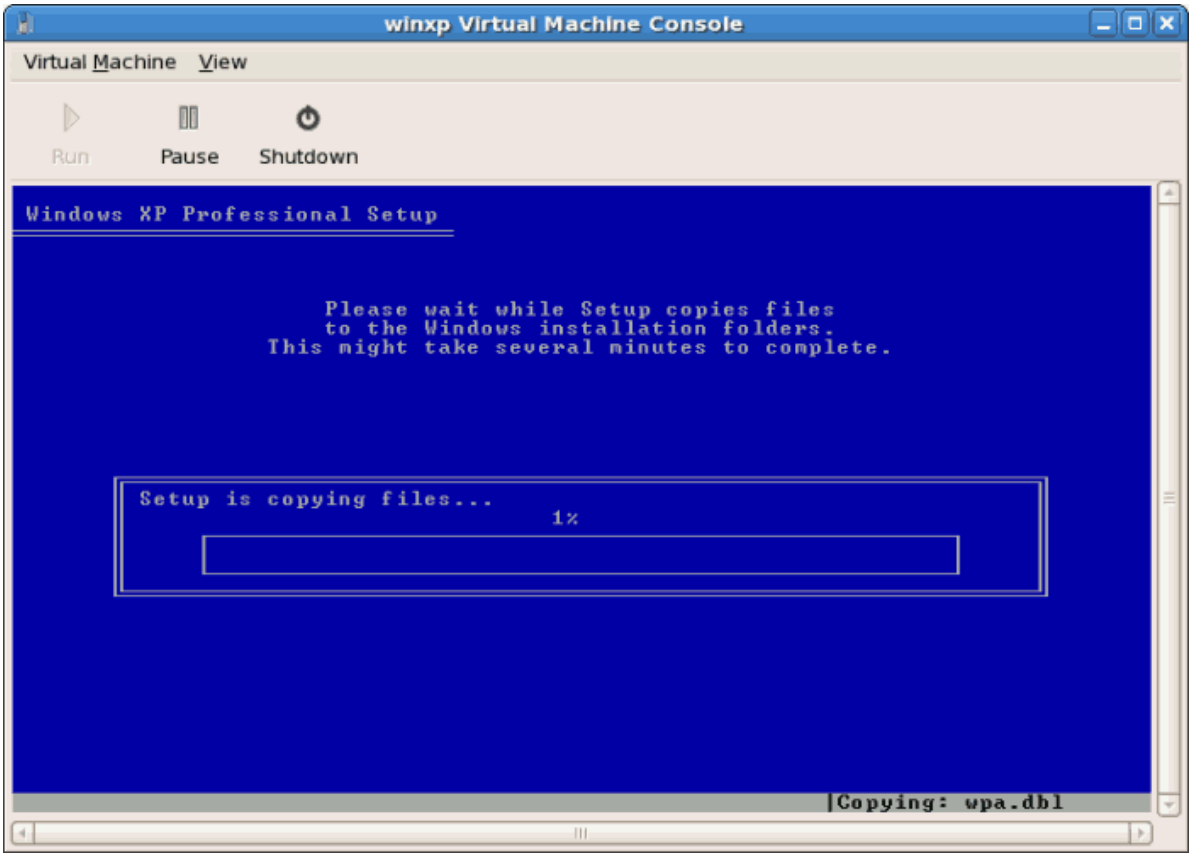

winxp Virtual Machine Console
Virtual Machine View
Run
Pause
Shutdown
Windows XP Licensing Agreement
END-USER LICENSE AGREEMENT FOR MICROSOFT SOFTWARE
WINDOWS XP PROFESSIONAL EDITION SERVICE PACK 2
IMPORTANT-READ CAREFULLY:
This End-User License Agreement ("EULA") is a legal agreement
between you (either an individual or a single entity) and
Microsoft Corporation or one of its affiliates ("Microsoft")
for the Microsoft software that accompanies this EULA, which
includes computer software and may include associated media,
printed materials, "online" or electronic documentation, and
Internet-based services ("Software"). An amendment or
addendum to this EULA may accompany the Software.
YOU AGREE TO BE BOUND BY THE TERMS OF THIS
EULA BY INSTALLING, COPYING, OR OTHERWISE
USING THE SOFTWARE. IF YOU DO NOT AGREE,
DO NOT INSTALL, COPY, OR USE THE SOFTWARE;
YOU MAY RETURN IT TO YOUR PLACE OF PURCHASE
FOR A FULL REFUND, IF APPLICABLE.
1. GRANT OF LICENSE.
Microsoft grants you the following rights provided that
you comply with all terms and conditions of this EULA:
1.1 Installation and use. You may install, use, access,
display and run one copy of the Software on a single
computer, such as a workstation, terminal or other
device ("Workstation Computer"). The Software may not
F8=I agree ESC=I do not agree PAGE DOWN=Next Page

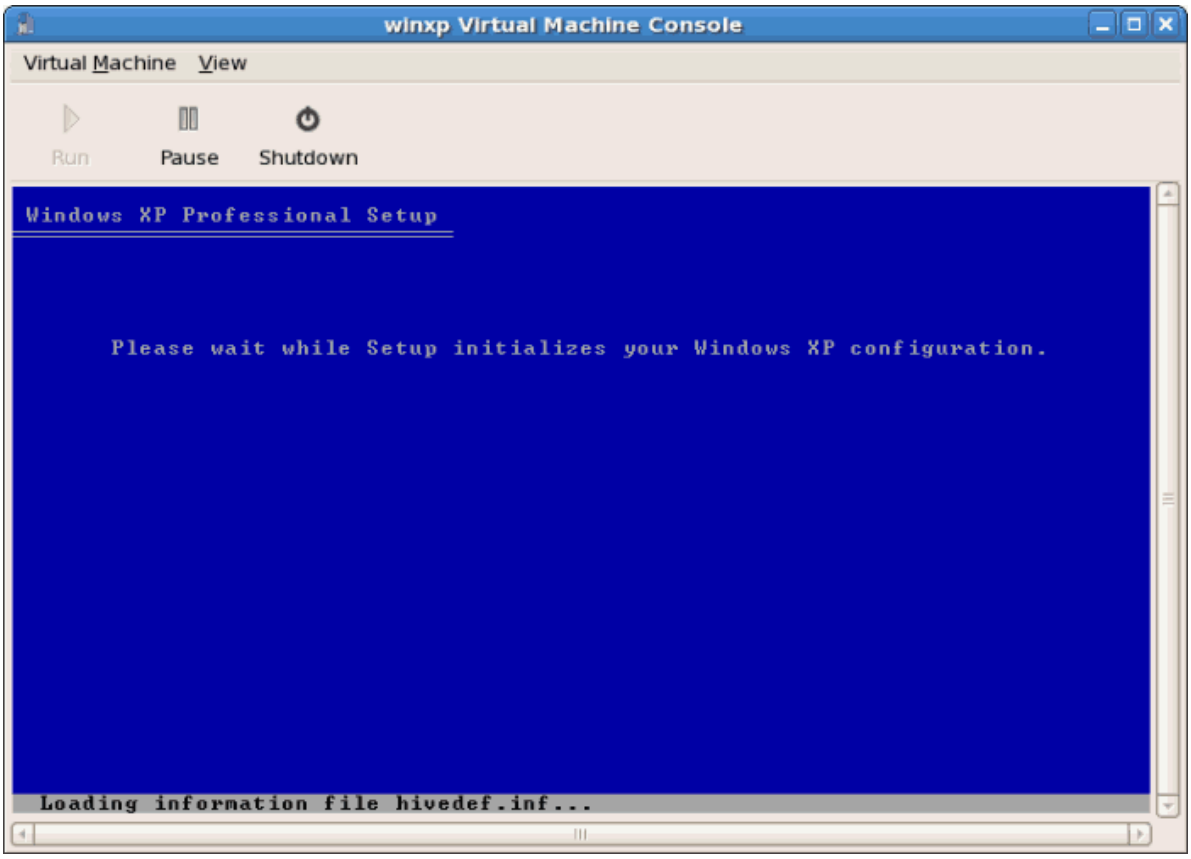
12. Divida el disco duro cuando se le solicite.


winxp Virtual Machine Console
Virtual Machine View
Run
Pause
Shutdown
Windows XP Professional Setup
The following list shows the existing partitions and unpartitioned space on this computer.
Use the UP and DOWN ARROW keys to select an item in the list.
• To set up Windows XP on the selected item, press ENTER.
• To create a partition in the unpartitioned space, press C.
• To delete the selected partition, press D.
3997 MB Disk 0 at Id 0 on bus 0 on atapi [MBR]
Unpartitioned space 3997 MB
ENTER=Install C=Create Partition F3=Quit

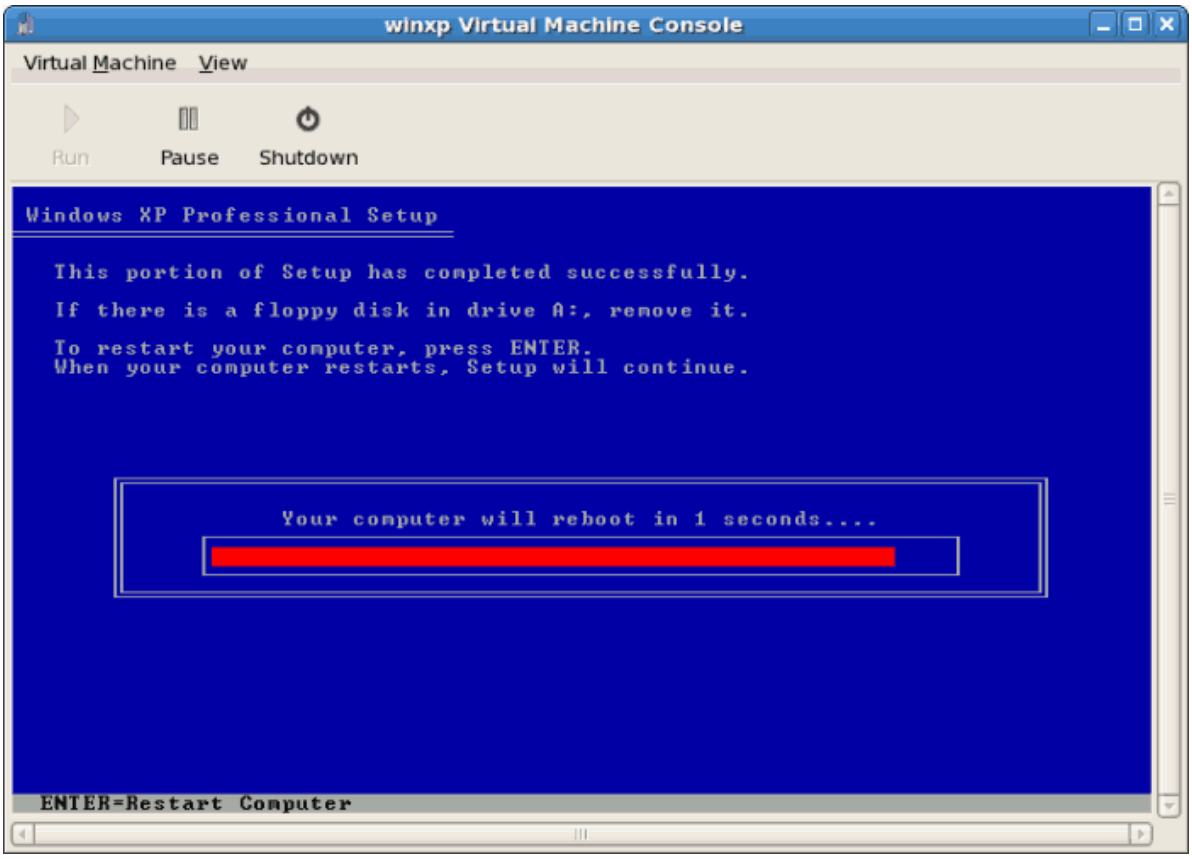

winxp Virtual Machine Console
Virtual Machine View
Run
Pause
Shutdown
Windows XP Professional Setup
A new partition for Windows XP has been created on
3997 MB Disk 0 at Id 0 on bus 0 on atapi [MBR].
This partition must now be formatted.
From the list below, select a file system for the new partition.
Use the UP and DOWN ARROW keys to select the file system you want,
and then press ENTER.
If you want to select a different partition for Windows XP,
press ESC.
Format the partition using the NTFS file system (Quick)
Format the partition using the FAT file system (Quick)
Format the partition using the NTFS file system
Format the partition using the FAT file system
ENTER=Continue ESC=Cancel

13. Luego que el disco haya sido formateado, Windows comienza a copiar los archivos en el disco rígido.





14. Los archivos son copiados al dispositivo de almacenamiento y ahora Windows reinicia.

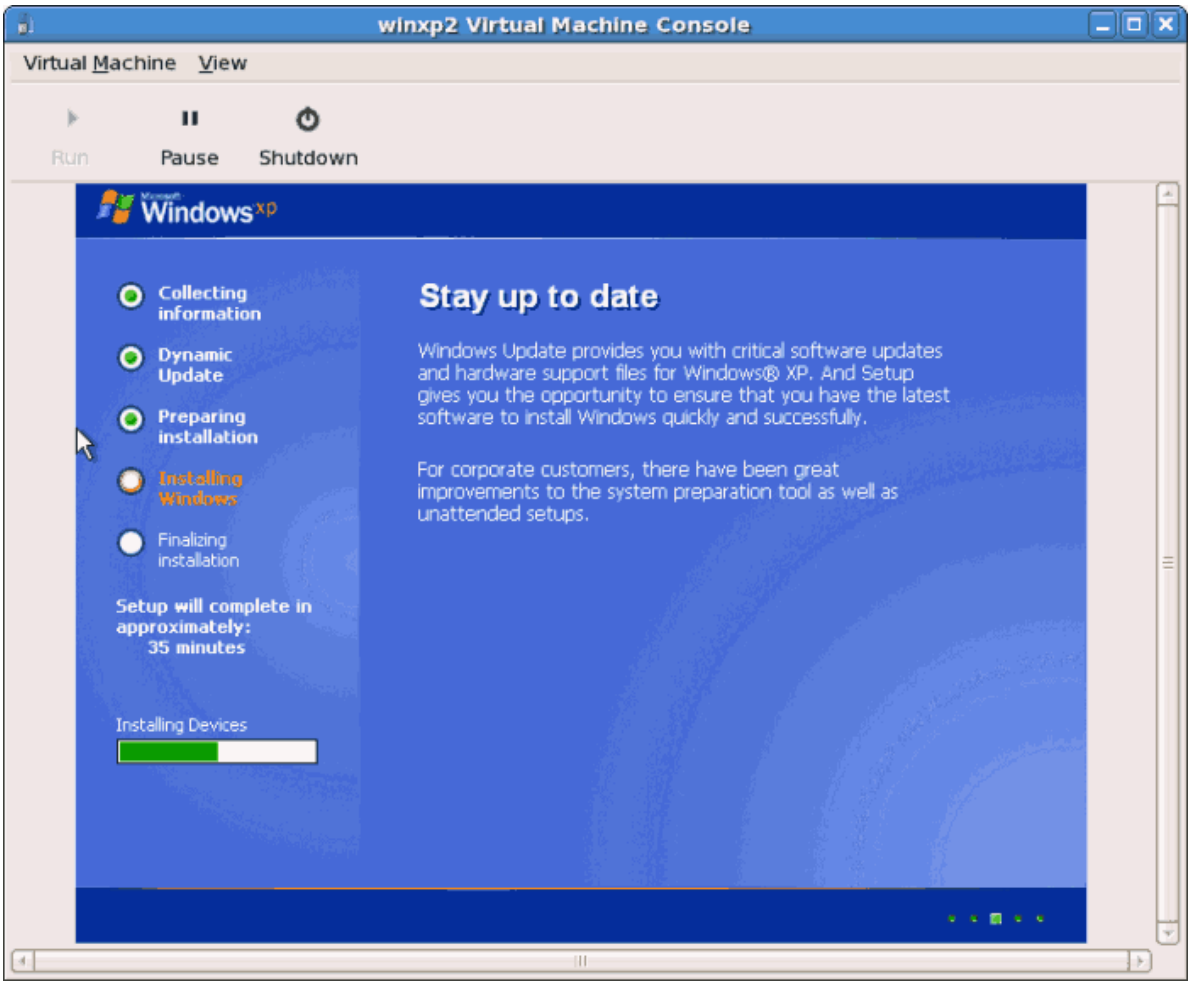

winxp Virtual Machine Console
Virtual Machine View
Run
Pause
Shutdown
Windows XP Professional Setup
This portion of Setup has completed successfully.
If there is a floppy disk in drive A:, remove it.
To restart your computer, press ENTER.
When your computer restarts, Setup will continue.
Your computer will reboot in 1 seconds....
ENTER=Restart Computer

15. Reinicie su huésped de Windows:

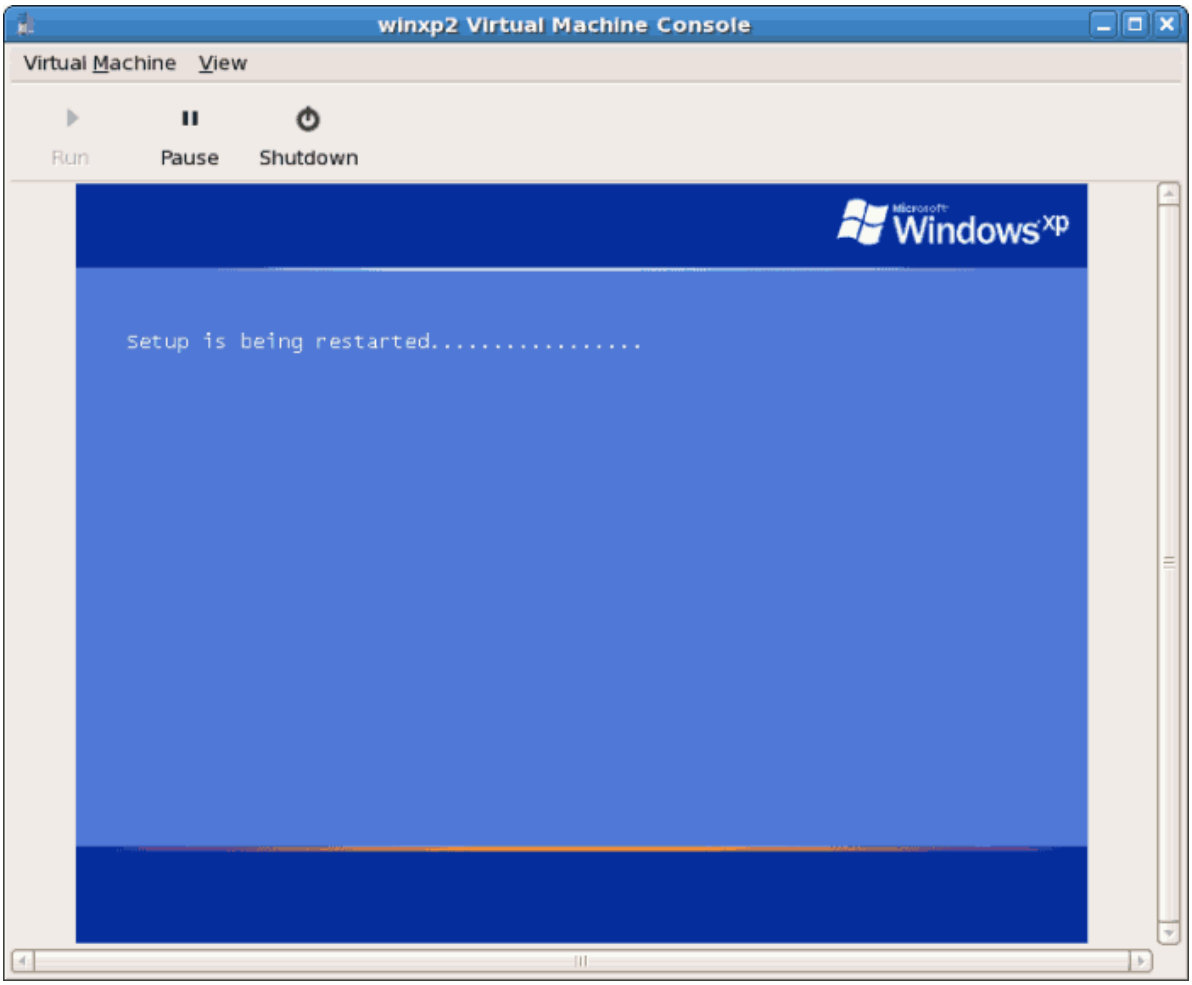
```
# virsh start WindowsGuest
```

Donde *WindowsGuest* es el nombre de su máquina virtual.

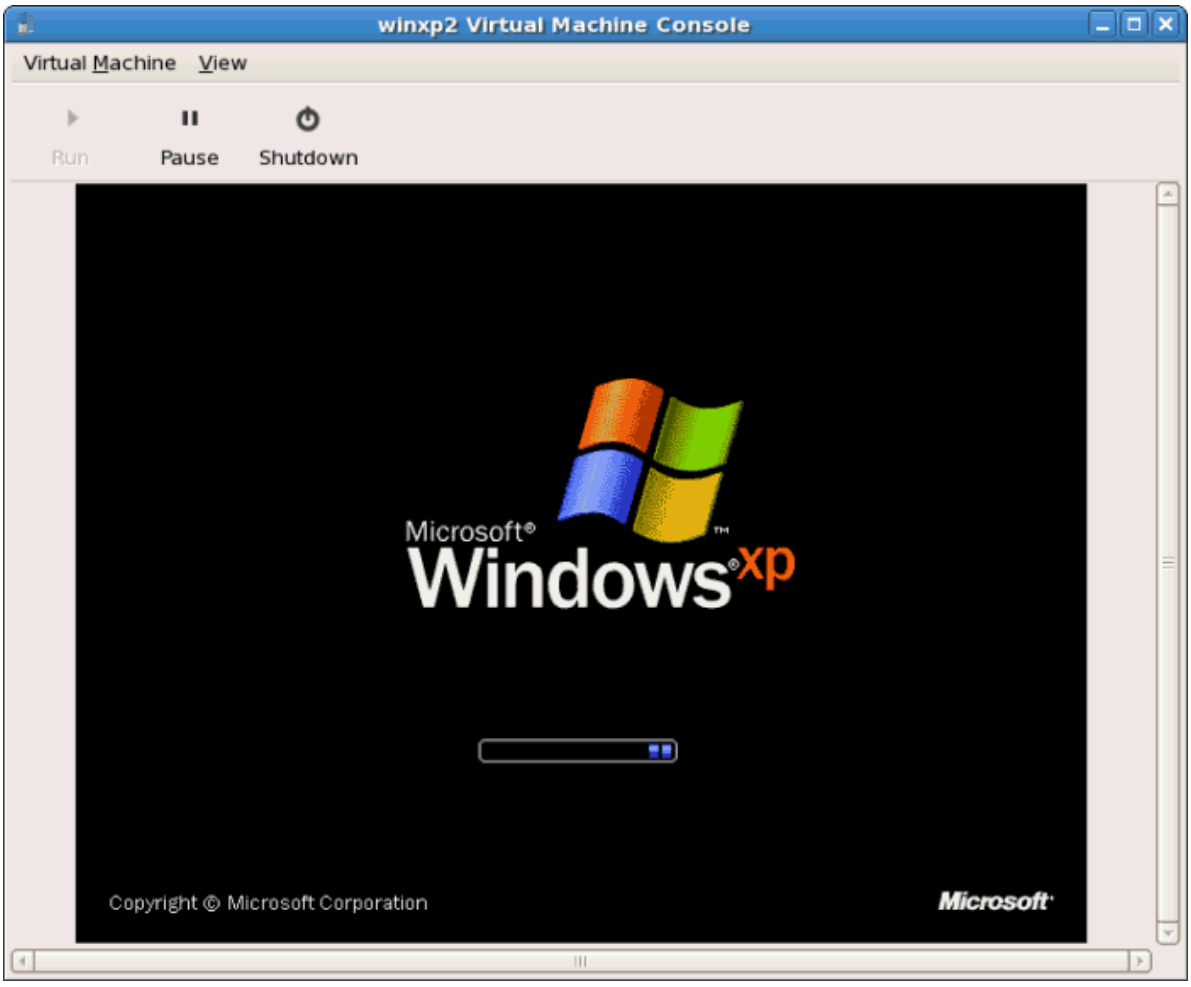
16. Cuando la ventana de consola se abre, verá la fase de configuración de la instalación de Windows.


winxp2 Virtual Machine Console
Virtual Machine View
Run
Pause
Shutdown
Windows xp
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete in approximately:
35 minutes
Installing Devices
Stay up to date
Windows Update provides you with critical software updates and hardware support files for Windows® XP. And Setup gives you the opportunity to ensure that you have the latest software to install Windows quickly and successfully.
For corporate customers, there have been great improvements to the system preparation tool as well as unattended setups.

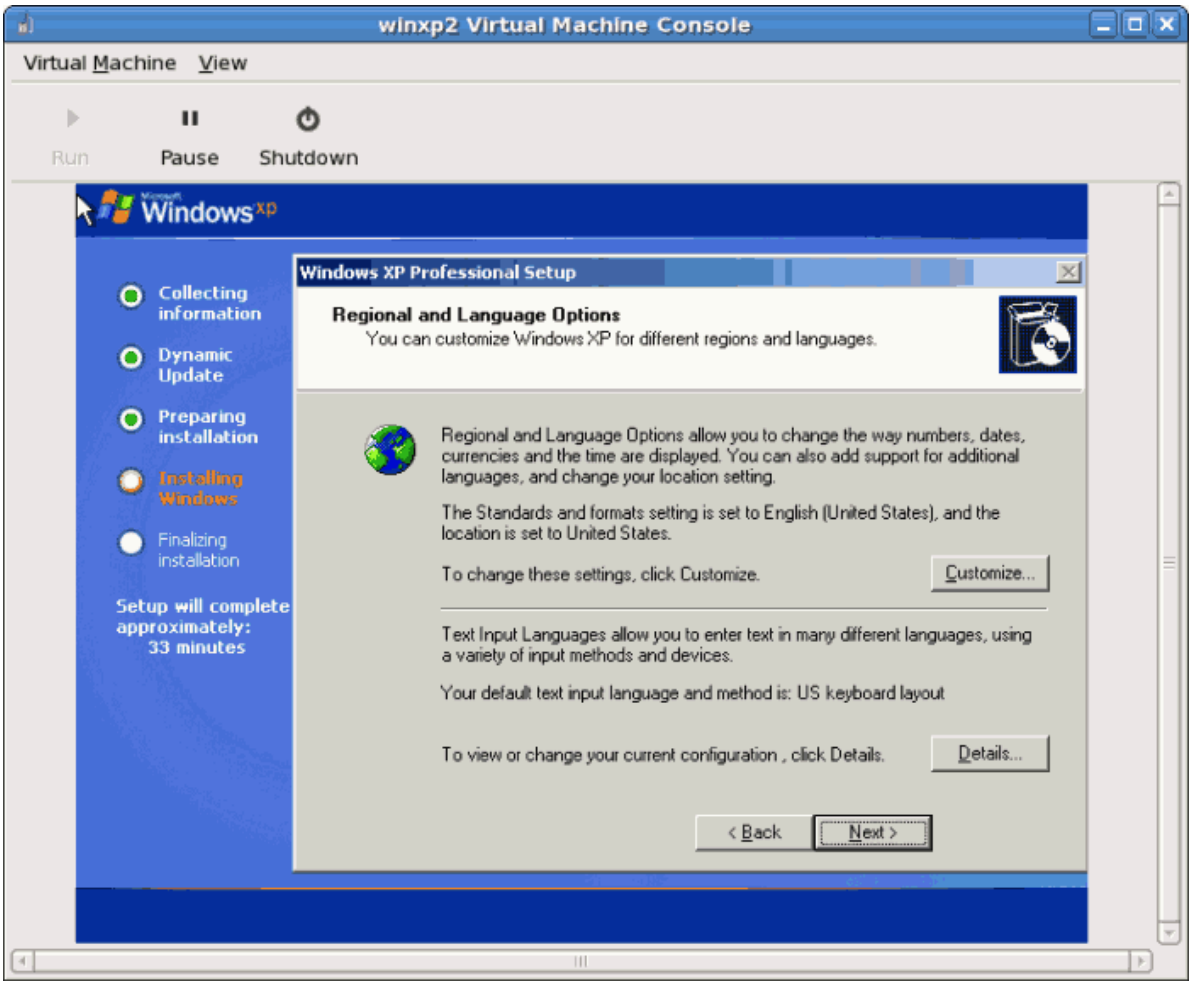
17. Si su instalación parece quedar trabada durante la fase de configuración, reinicie el huésped con **`virsh reboot` *`NombreDelHuéspedWindows`***. Cuando reinicie la máquina virtual verá el mensaje **`Setup is being restarted`**:



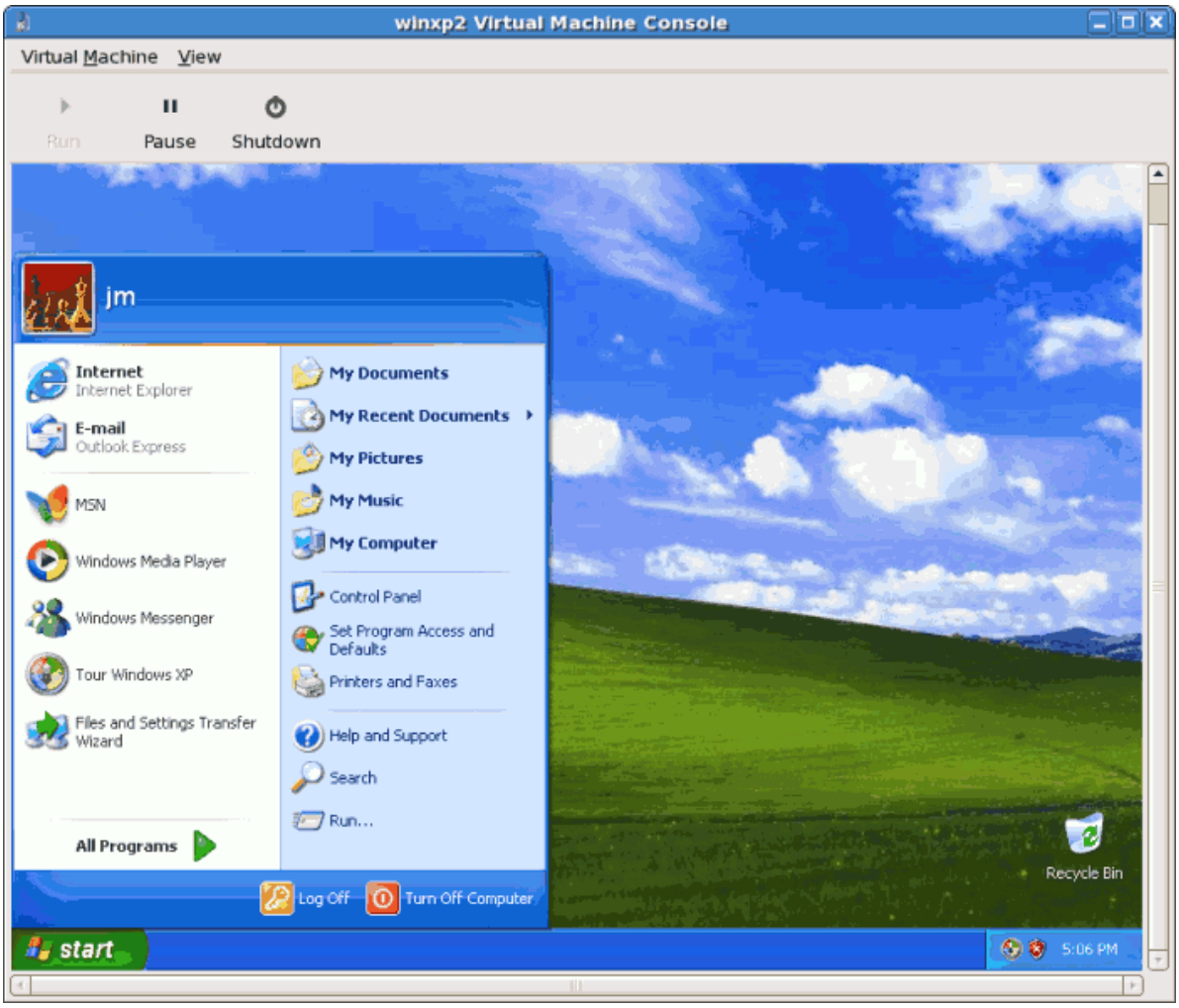
18. Cuando la configuración ha terminado, verá la pantalla de arranque de Windows:



19. Ahora, puede continuar con la configuración estándar de su instalación de Windows:


winxp2 Virtual Machine Console
Virtual Machine View
Run
Pause
Shutdown
Windows XP
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete approximately: 33 minutes
Windows XP Professional Setup
Regional and Language Options
You can customize Windows XP for different regions and languages.
Regional and Language Options allow you to change the way numbers, dates, currencies and the time are displayed. You can also add support for additional languages, and change your location setting.
The Standards and formats setting is set to English (United States), and the location is set to United States.
To change these settings, click Customize.
Customize...
Text Input Languages allow you to enter text in many different languages, using a variety of input methods and devices.
Your default text input language and method is: US keyboard layout
To view or change your current configuration , click Details.
Details...
< Back
Next >

20. El proceso de configuración ha sido completado.


winxp2 Virtual Machine Console
Virtual Machine View
Run
Pause
Shutdown
jm
Internet
Internet Explorer
E-mail
Outlook Express
MSN
Windows Media Player
Windows Messenger
Tour Windows XP
Files and Settings Transfer Wizard
All Programs
My Documents
My Recent Documents
My Pictures
My Music
My Computer
Control Panel
Set Program Access and Defaults
Printers and Faxes
Help and Support
Search
Run...
Log Off
Turn Off Computer
Recycle Bin
start
5:06 PM

Instalación de Windows Server 2003 como un huésped completamente virtualizado

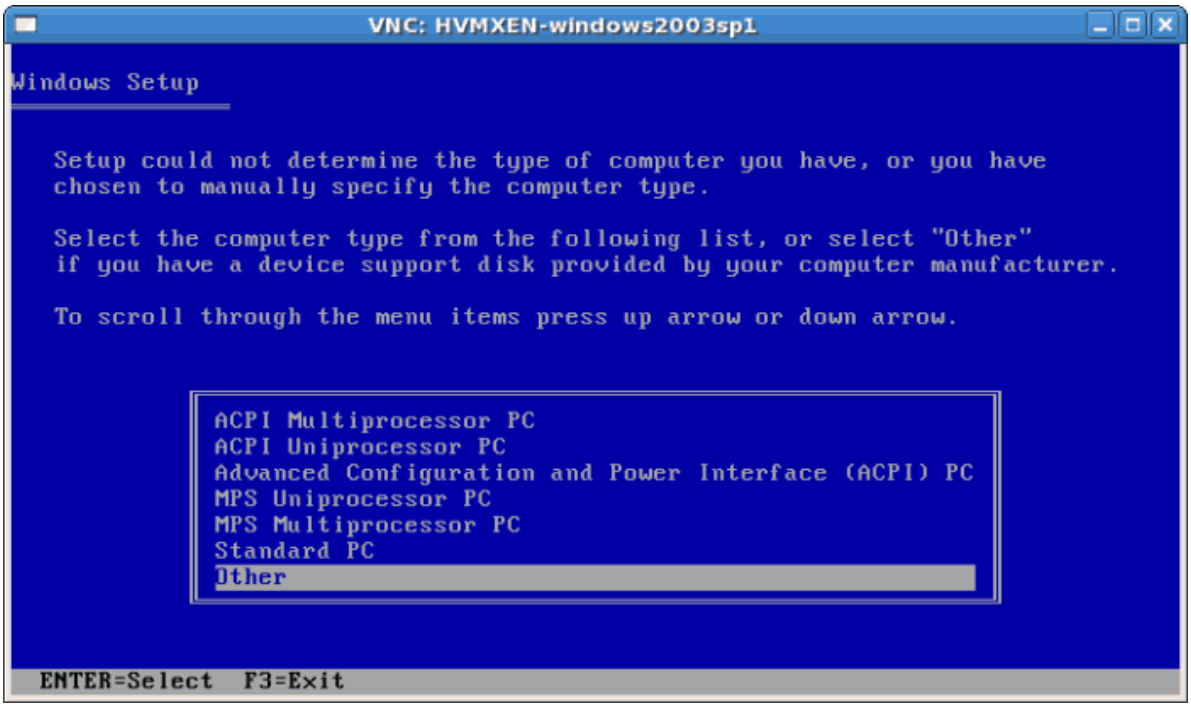
Este capítulo describe la instalación de un huésped completamente virtualizado de Windows Server 2003, mediante la utilización del comando **`virt-install`**. Este comando puede utilizarse en lugar de **`virt-manager`**. Este proceso es similar a la instalación Windows XP descrita en*Capítulo 7, Instalación de Windows XP como huésped completamente virtualizado*.

1. El uso de **`virt-install`** para instalar Windows Server 2003 como consola para el huésped de Windows, hace que se abre la ventana **`virt-viewer`**. El ejemplo que ofrecemos a continuación instala un huésped de Windows Server 2003 con el comando **`virt-install`**.

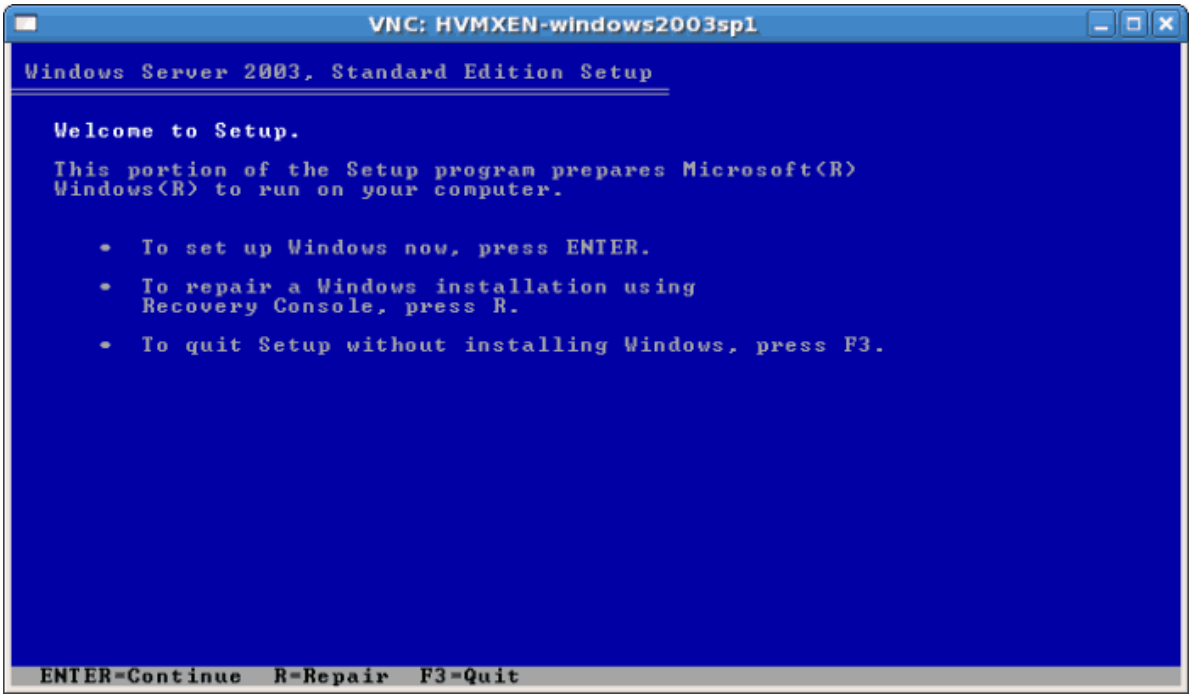
```
# virt-install --accelerate --hvm --connect qemu:///system \
   --name rhel3support  \
   --network network:default \
   --file=/var/lib/libvirt/images/windows2003sp2.img \
   --file-size=6 \
   --cdrom=/var/lib/libvirt/images/ISOs/WIN/en_windows_server_2003_sp1.iso \
   --vnc --ram=1024
```

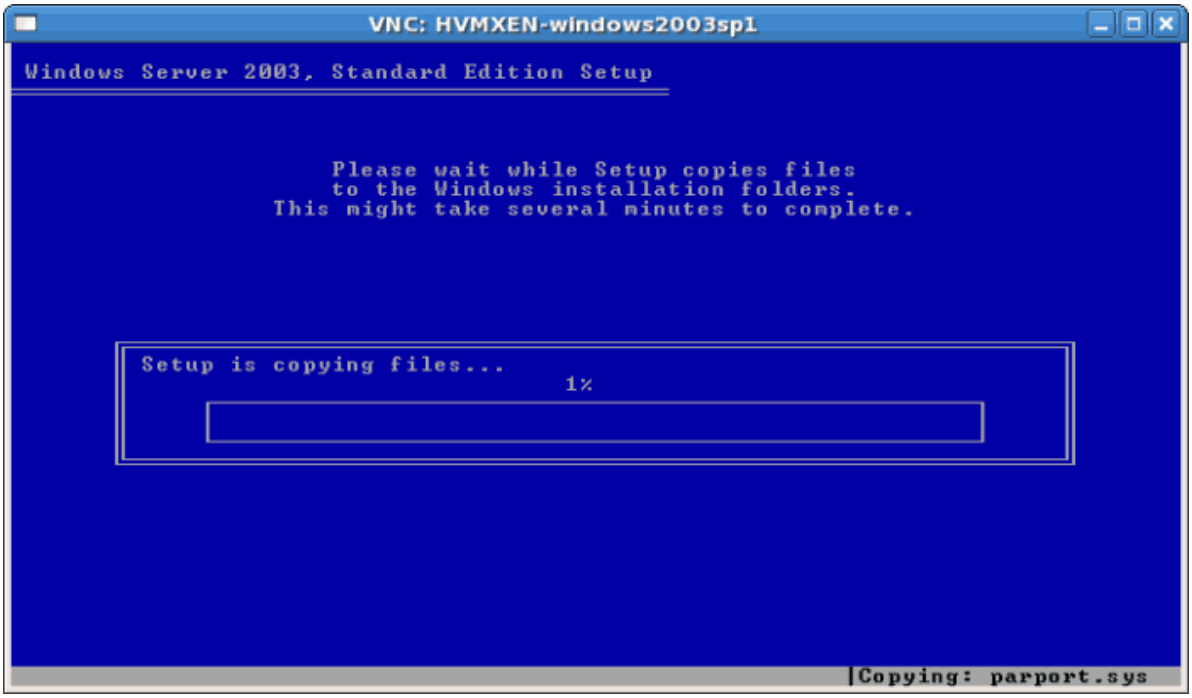
Ejemplo 8.1. virt-install de KVM

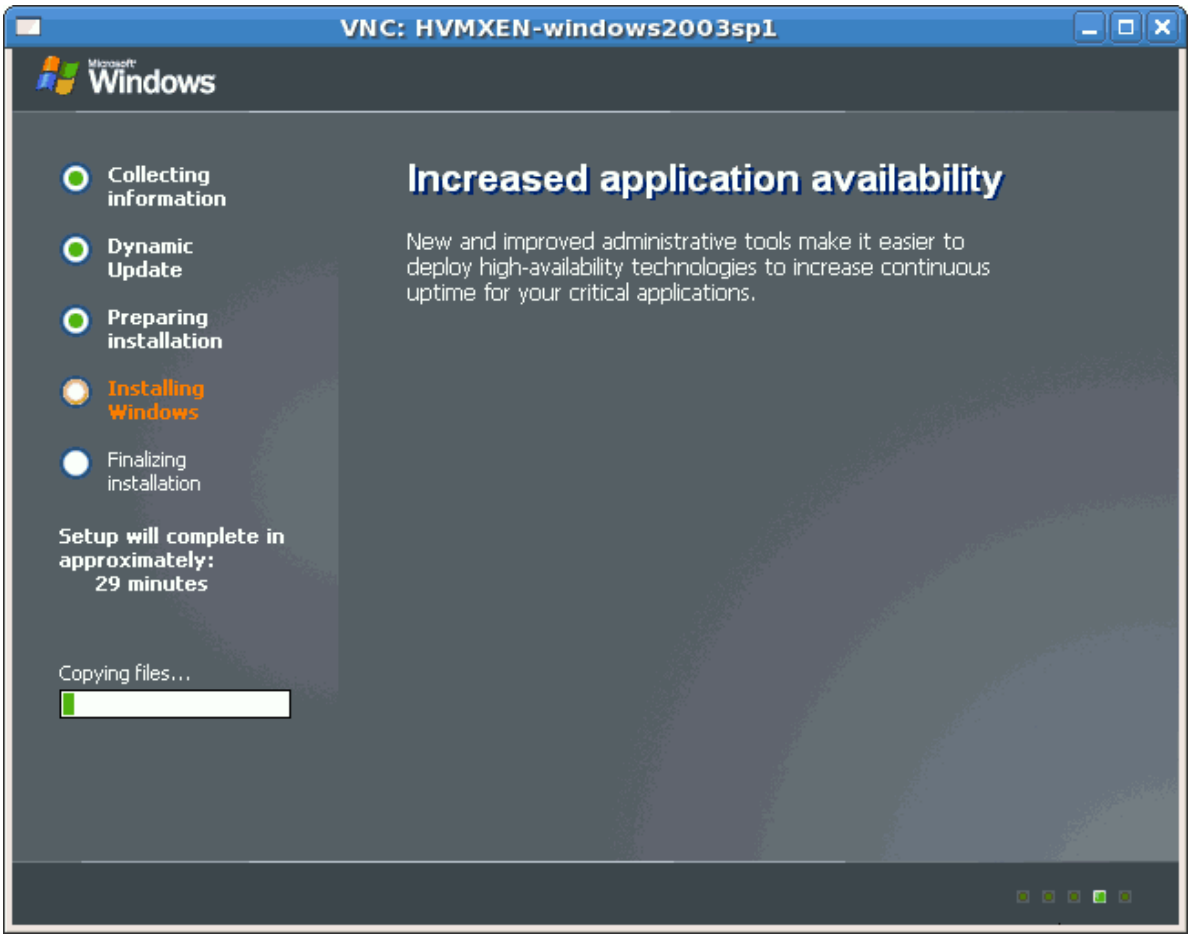
2. Una vez que el huésped arranca dentro de la instalación, se debe presionar rápidamente **F5**. Si no lo hace en el momento preciso, necesitará reiniciar la instalación. El presionar la tecla **F5** le permite elegir entre diferentes **HAL** o **Tipo de computadora**. Elija **`Standard PC`** como el **Tipo de computadora**. Modificar el **Tipo de computadora** es necesario para los huéspedes virtualizados de Windows Server 2003.


VNC: HVMXEN-windows2003sp1
Windows Setup
Setup could not determine the type of computer you have, or you have chosen to manually specify the computer type.
Select the computer type from the following list, or select "Other" if you have a device support disk provided by your computer manufacturer.
To scroll through the menu items press up arrow or down arrow.
ACPI Multiprocessor PC
ACPI Uniprocessor PC
Advanced Configuration and Power Interface (ACPI) PC
MPS Uniprocessor PC
MPS Multiprocessor PC
Standard PC
Other
ENTER=Select F3=Exit

3. Complete el resto de la instalación.


VNC: HVMXEN-windows2003sp1
Windows Server 2003, Standard Edition Setup
Welcome to Setup.
This portion of the Setup program prepares Microsoft(R)
Windows(R) to run on your computer.
• To set up Windows now, press ENTER.
• To repair a Windows installation using
Recovery Console, press R.
• To quit Setup without installing Windows, press F3.
ENTER=Continue R=Repair F3=Quit


VNC: HVMXEN-windows2003sp1
Windows Server 2003, Standard Edition Setup
Please wait while Setup copies files
to the Windows installation folders.
This might take several minutes to complete.
Setup is copying files...
1%
Copying: parport.sys



4. Ahora, Windows Server 2003 está instalado como huésped completamente virtualizado.

Installing Windows Server 2008 como huésped totalmente virtualizado

Esta sección detalla la instalación de un huésped Windows Server 2008 completamente virtualizado sobre Fedora.

Procedimiento 9.1. Instalación de Windows Server 2008 con virt-manager

1. **Inicie virt-manager**
   Inicie **`virt-manager`**: Abra la herramienta **Administrador de máquinas virtuales** desde el menú **Aplicaciones** y **Herramientas del sistema**. De forma alternativa, ejecute el comando **`virt-manager`** como usuario root.

2. **Seleccione un hipervisor**
   Seleccione el hipervisor. Tenga en cuenta que actualmente, el hipervisor KVM es denominado **`qemu`**.

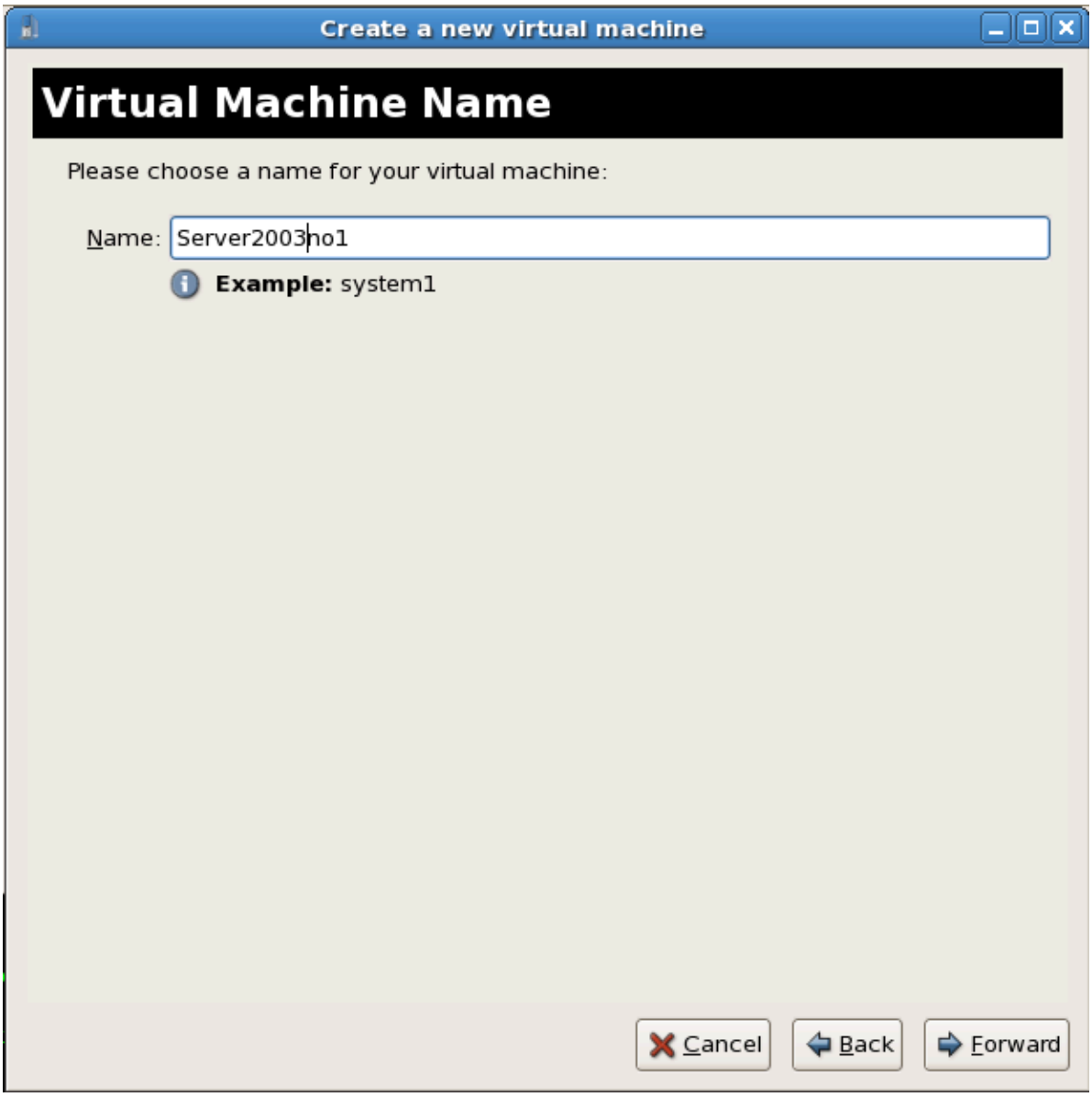
   Una vez seleccionada esta opción el botón **Nuevo** aparece. Presione el botón **Nuevo**.

3. **Inicie el asistente de nueva máquina virtual**
   Al presionar el botón de **Nuevo**, se inicia el asistente para generar una nueva máquina virtual.

Create a new virtual machine
Virtual Machine Creation
This assistant will guide you through creating a new virtual machine. You will be asked for some information about the virtual machine you'd like to create, such as:
A name for your new virtual machine
Whether the virtual machine will be fully virtualized or para-virtualized
The location of the files necessary for installing an operating system on the virtual machine
Storage details - which disk partitions or files the virtual machine should use
Memory and CPU allocation
Cancel
Back
Forward

Presione **Adelante** para continuar.

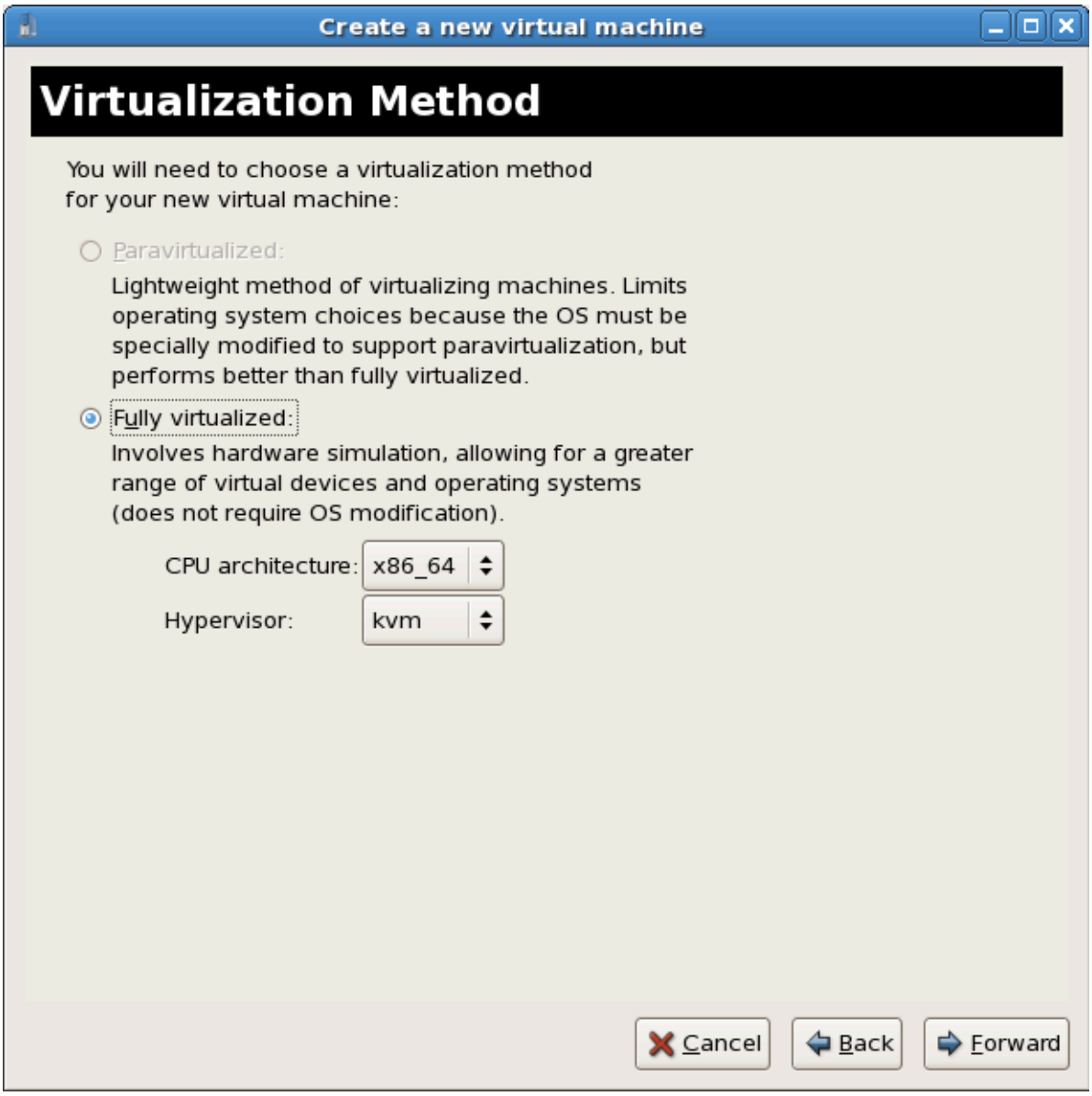
4. **Identifique al huésped con un nombre**
   The following characters are allowed in guest names: '_', '**.**' and '**-**' characters.



Presione **Avanzar** para continuar.

5. **Elija un método de virtualización**
   Aparece la ventana de **Elija un método de virtualización**

   Una virtualización completa necesita un procesar con las extensiones AMD 64 y AMD-V, o un procesador con las extensiones Intel 64 e Intel VT. Si las extensiones de virtualización no se encuentran presentes, KVM no estará disponible.


Create a new virtual machine
Virtualization Method
You will need to choose a virtualization method for your new virtual machine:
Paravirtualized:
Lightweight method of virtualizing machines. Limits operating system choices because the OS must be specially modified to support paravirtualization, but performs better than fully virtualized.
Fully virtualized:
Involves hardware simulation, allowing for a greater range of virtual devices and operating systems (does not require OS modification).
CPU architecture: x86_64
Hypervisor: kvm
Cancel
Back
Forward

Presione **Avanzar** para continuar.

6. **Seleccione el método de instalación**
   Para todas las versiones de Windows, debe usar **local install media**, ya sea una imagen ISO o un medio óptico físico.

   PXE puede usarse si ya se tiene un servidor PXE para instalación de red de Windows. La instalación PXE Windows no se cubre en este manual.

   Defina el **Tipo de SO** para **Windows**, con la **Variante** para **Microsoft Windows 2008** como se muestra en la captura de pantalla.

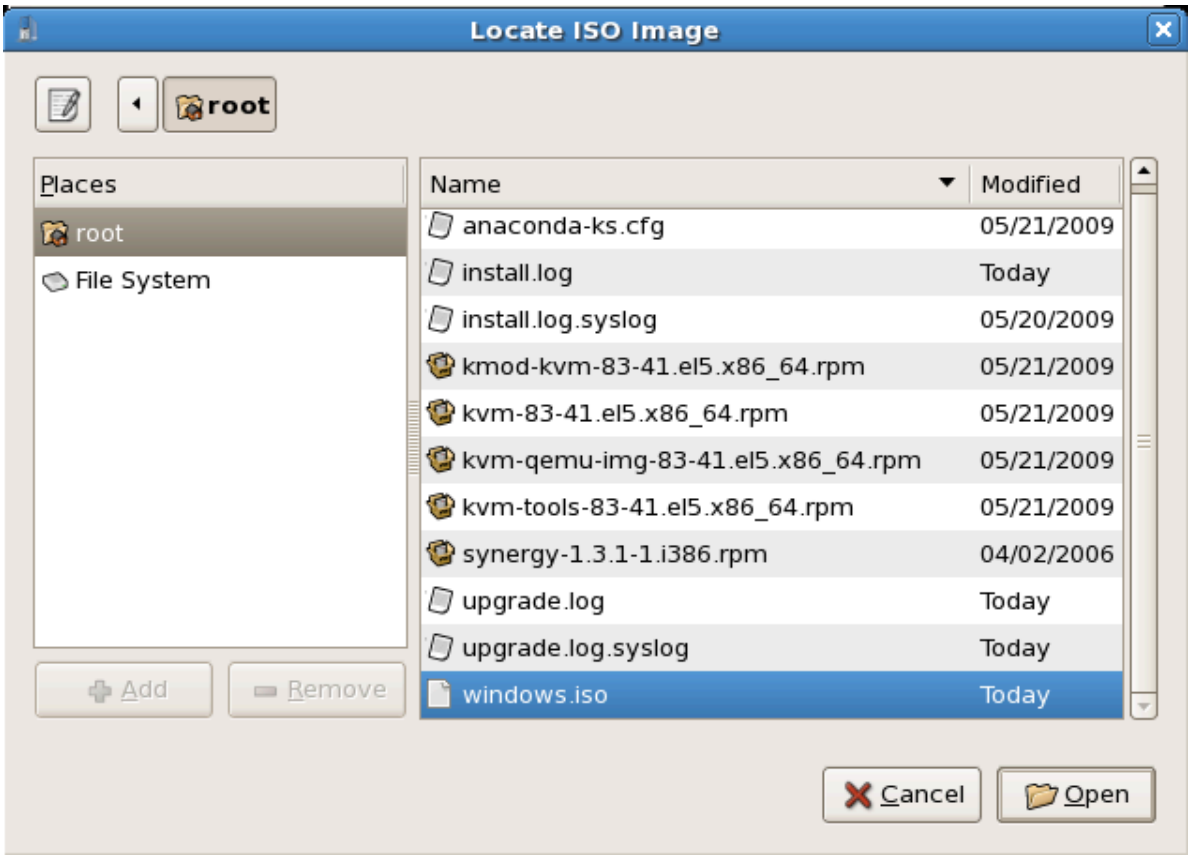
Create a new virtual machine
Installation Method
Please indicate where installation media is available for the operating system you would like to install on this virtual machine:
Local install media (ISO image or CDROM)
Network install tree (HTTP, FTP, or NFS)
Network boot (PXE)
Please choose the operating system you will be installing on the virtual machine:
OS Type: Windows
OS Variant: Microsoft Windows 2008
Cancel
Back
Forward

Presione **Adelante** para continuar.

7. **Ubique el medio de instalación**
   Seleccione la ubicadión de la imagen ISO o CD-ROM o el dispositivo DVD. Este ejemplo utiliza una imagen de archivo ISO del CD de instalación de Windows Server 2008.

   a. Haga clic en el botón **Browse**.

   b. Busque la ubicación del archivo ISO y selecciónelo.



Presione **Abrir** para confirmar su elección.

c. El archivo está seleccionado y listo para ser instalado.

Presione **Adelante** para continuar.

Archivos de imagen y SELinux

Para archivos de imagen ISO, e imágenes de almacenamiento de huésped, se recomienda utilizar el directorio **`/var/lib/libvirt/images/`**. Cualquier otra ubicación puede requerir una configuración adicional para SELinux. Para obtener mayor información, consulte*Sección 19.2, "SELinux y virtualización completas"*.

8. **Configuración del almacenamiento**

   Asigne un dispositivo de almacenamiento físico (**Dispositivos de bloque**) o una imagen basada en archivo (**Archivo**). Las imágenes basadas en archivos deben ser almacenadas en el directorio **`/var/lib/libvirt/images/`**. Asigne espacio suficiente para el almacenamiento de su huésped virtualizado, y para cualquier aplicación que éste necesite.

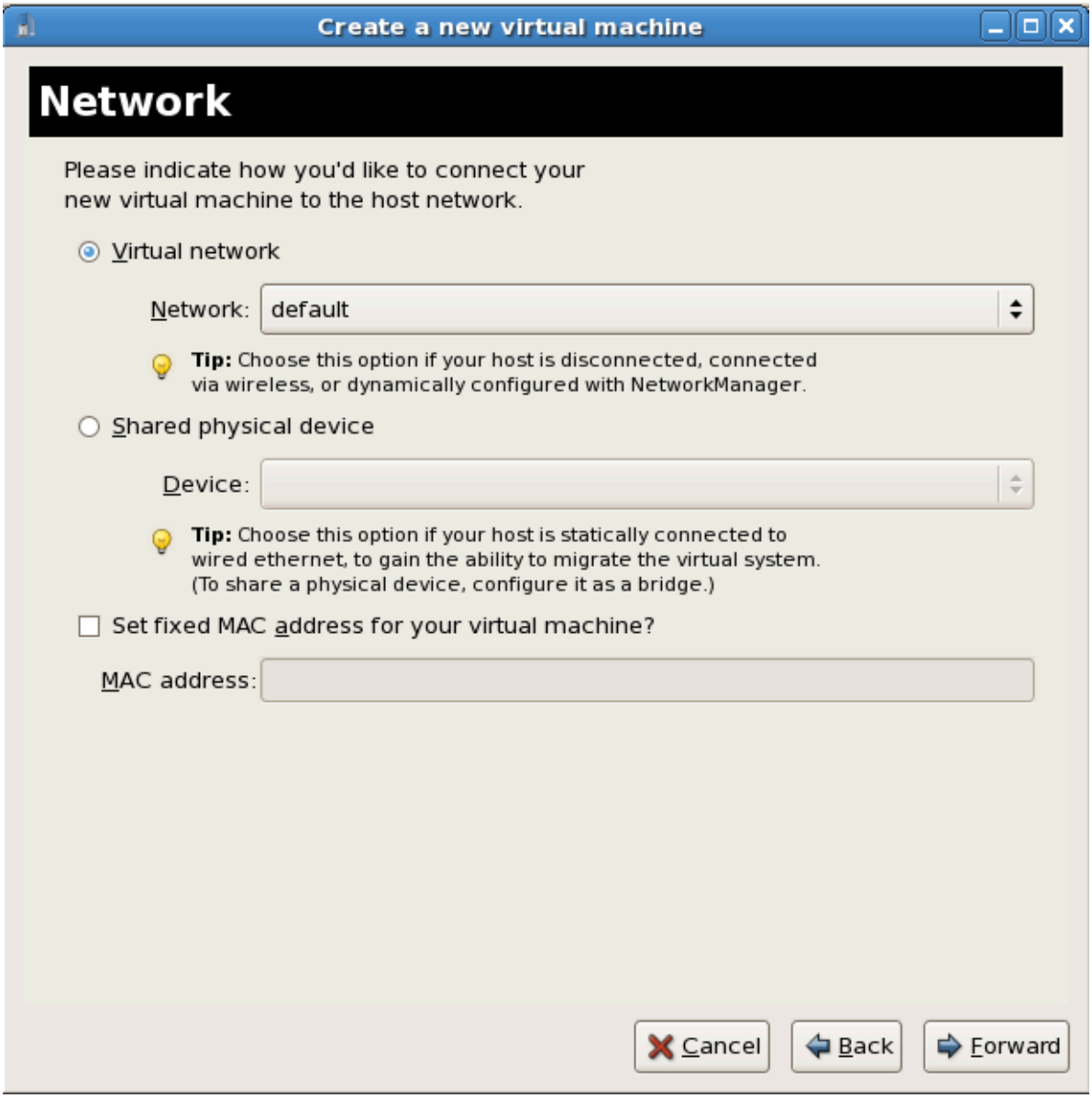
Create a new virtual machine
Storage
Please indicate how you'd like to assign space from the host for your new virtual machine. This space will be used to install the virtual machine's operating system.
Block device (partition):
Location:
Browse...
Example: /dev/hdc2
File (disk image):
Location: /var/lib/libvirt/images/Server2008r
Browse...
Size: 7000 MB
Allocate entire virtual disk now
Warning: If you do not allocate the entire disk now, space will be allocated as needed while the virtual machine is running. If sufficient free space is not available on the host, this may result in data corruption on the virtual machine.
Tip: You may add additional storage, including network-mounted storage, to your virtual machine after it has been created using the same tools you would on a physical system.
Cancel
Back
Forward

Presione **Adelante** para continuar.

9. **Configuración de la red**
   Elija o bien **Red virtual**, o bien **DIspositivo físico compartido**.

   La opción de red virtual utiliza el protocolo de Traducción de direcciones de red (NAT, por las iniciales en inglés de Network Address Translation) para poder compartir el dispositivo de red predeterminado con los huéspedes virtualizados. Utilice la opción de red virtual para redes inalámbricas.

   La opción de dispositivo físico compartido utiliza un enlace de red para otorgarle al huésped virtualizado un acceso completo al dispositivo de red


Create a new virtual machine
Network
Please indicate how you'd like to connect your new virtual machine to the host network.
Virtual network
Network: default
Tip: Choose this option if your host is disconnected, connected via wireless, or dynamically configured with NetworkManager.
Shared physical device
Device:
Tip: Choose this option if your host is statically connected to wired ethernet, to gain the ability to migrate the virtual system. (To share a physical device, configure it as a bridge.)
Set fixed MAC address for your virtual machine?
MAC address:
Cancel
Back
Forward

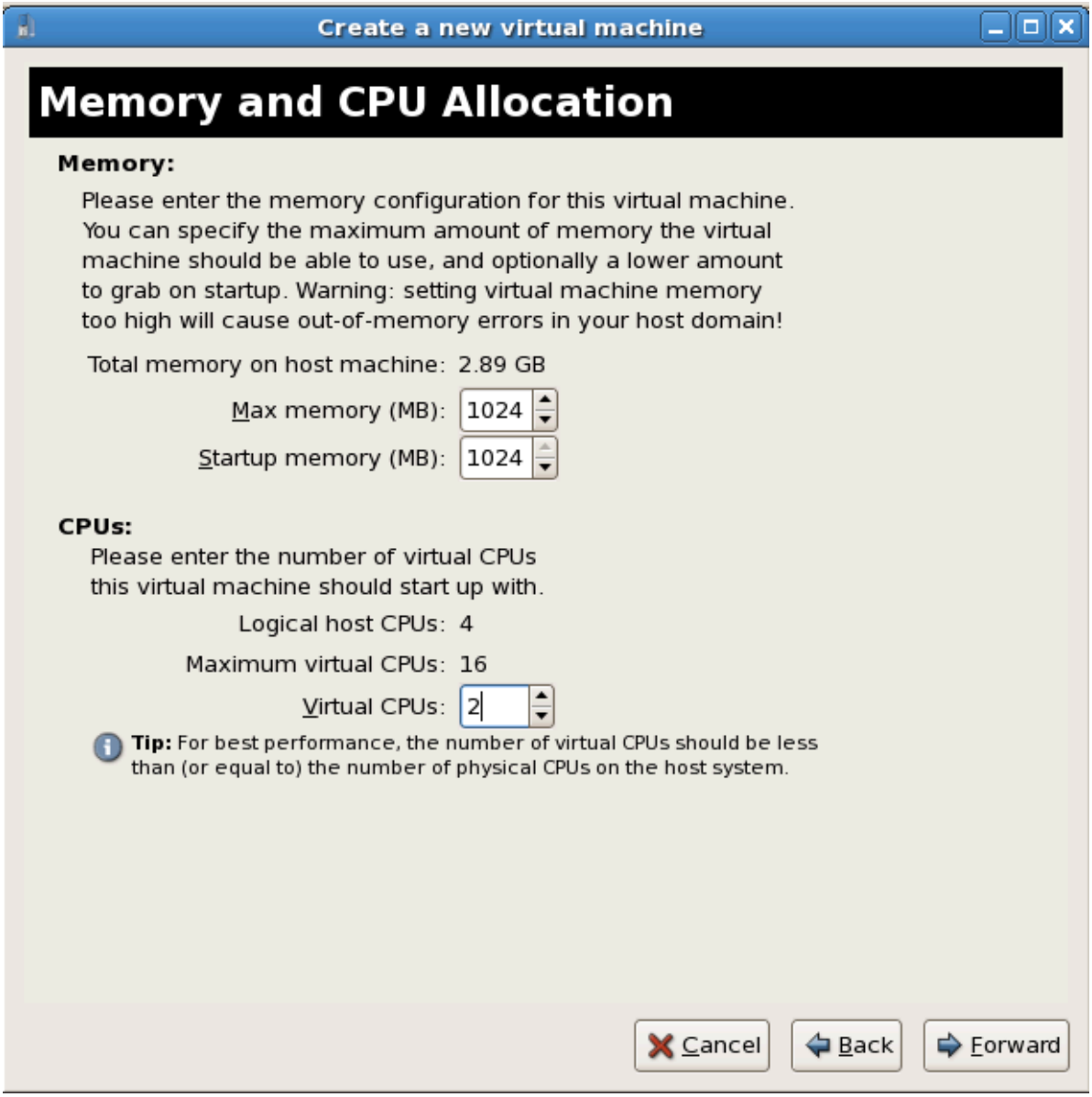
Presione **Adelante** para continuar.

10. **Alojamiento de la memoria y del CPU**
    The **Memory and CPU Allocation** window displays. Choose appropriate values for the virtualized CPUs and RAM allocation. These values affect the host's and guest's performance.

    Los huéspedes virtualizados requieren de suficiente memoria física (RAM) para ejecutarse eficiente y eficazmente. Elija una valor de memoria apto para los requerimientos de su sistema operativo huésped, y para sus aplicaciones. Recuerde que los huéspedes utilizan RAM física. La ejecución de demasiados huéspedes, o destinar un resto de memoria insuficiente para el sistema del equipo anfitrión, causará una utilización significativa de la memoria virtual y del espacio de intercambio. La memoria virtual es notoriamente más lenta, y esto hace que el rendimiento y receptividad del sistema se degrade. Asegúrese de asignar suficiente memoria para que todos los huéspedes y el equipo anfitrión operen de modo eficaz.

    Asigne suficientes CPUs virtuales para el huésped virtualizado. Si el huésped ejecuta una aplicación múltiple, asigne la cantidad de CPUs virtuales necesarias para que el huésped

se ejecute de manera apropiada. No asigne mayor cantidad de CPUs virtuales, que la de procesadores físicos disponibles en el equipo anfitrión. Si bien es posible sobrealojar procesadores virtuales, el sobrealojamiento tiene un efecto significativo y negativo sobre el desempeño tanto del equipo como de los huéspedes. Esto es debido al contexto de intercambio de procesos generales del procesador.

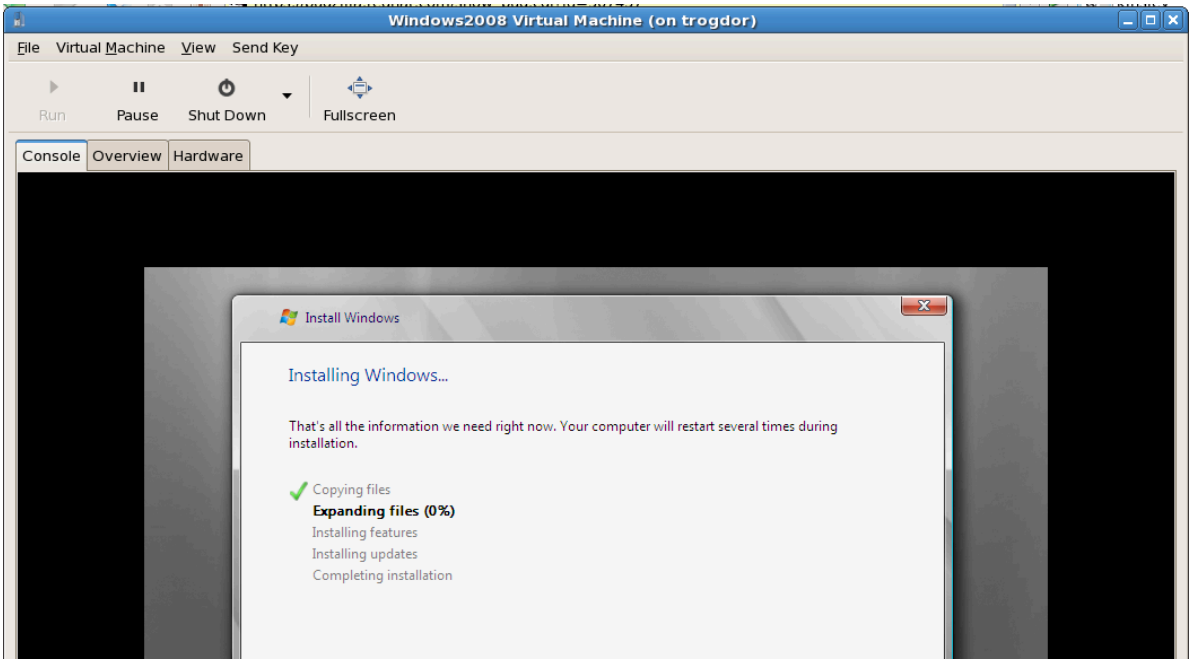

Create a new virtual machine
Memory and CPU Allocation
Memory:
Please enter the memory configuration for this virtual machine. You can specify the maximum amount of memory the virtual machine should be able to use, and optionally a lower amount to grab on startup. Warning: setting virtual machine memory too high will cause out-of-memory errors in your host domain!
Total memory on host machine: 2.89 GB
Max memory (MB): 1024
Startup memory (MB): 1024
CPUs:
Please enter the number of virtual CPUs this virtual machine should start up with.
Logical host CPUs: 4
Maximum virtual CPUs: 16
Virtual CPUs: 2
Tip: For best performance, the number of virtual CPUs should be less than (or equal to) the number of physical CPUs on the host system.
Cancel
Back
Forward

Presione **Adelante** para continuar.

11. **Verifique y comience la instalación del huésped**
    Verifique la configuración.

Presione **Terminar** para iniciar el procedimiento de instalación del huésped.

12. **Instalación de Windows**


Windows2008 Virtual Machine (on trogdor)
File Virtual Machine View Send Key
Run Pause Shut Down Fullscreen
Console Overview Hardware
Install Windows
Installing Windows...
That's all the information we need right now. Your computer will restart several times during installation.
Copying files
Expanding files (0%)
Installing features
Installing updates
Completing installation

Complete the Windows Server 2008 installation sequence. The installation sequence is not covered by this guide, refer to Microsoft's *documentation*[1] for information on installing Windows.

Parte III. Configuración

Configuración de la virtualización en Fedora

Estos capítulos detallan los procedimientos de configuración para varias tareas avanzadas de virtualización. Estas tareas incluyen la adición de dispositivos de red y de almacenamiento, mejorar el rendimiento, y utilización de *controladores para-virtualizados* en huéspedes completamente para-virtualizados.

Dispositivos de almacenamiento virtualizados

Este capítulo trata sobre la instalación y configuración de dispositivos de almacenamiento en huéspedes virtualizados. El término dispositivos de bloque se refiere a varias formas de dispositivos de almacenamiento. Todos los procedimientos descritos en este capítulo funcionan tanto con el hipervisor KVM, como con el hipervisor Xen.

Dispositivos de disco válidos

La variable de dispositivos en el archivo de configuración de libvirt acepta solo los nombres que se muestran a continuación:

- **`/dev/xvd[de la 'a' hasta la 'z'][de 1 a 15]`**

  Por ejemplo: **`/dev/xvdb13`**

- **`/dev/xvd[de la 'a' hasta la 'i'][de la 'a' hasta la 'z'][de 1 a 15]`**

  Por ejemplo: **`/dev/xvdbz13`**

- **`/dev/sd[de la 'a' hasta la 'p'][de 1 a 15]`**

  Por ejemplo: **`/dev/sda1`**

- **`/dev/hd[de la 'a' hasta la 't'][de 1 a 63]`**

  Por ejemplo: **`/dev/hdd3`**

10.1. Cómo crear un controlador de disquete virtualizado

Los controladores de disquete son necesarios para una gran cantidad de sistemas operativos anteriores, especialmente en la instalación de controladores. Actualmente, los dispositivos de disquete no se pueden acceder desde huéspedes virtualizados. Sin embargo, la creación y el acceso a imágenes de disquete desde unidades de disquetes virtualizadas debería ser posible. Esta sección describe la creación de un dispositivo de disquete virtualizado.

Se necesita un archivo de imagen de un disquete. Cree archivos de imágenes de disquete con el comando **dd**. Remplace /dev/fd0 por el nombre de un disquete y dele el nombre apropiado al disco.

```
# dd if=/dev/fd0 of=~/legacydrivers.img
```

Este ejemplo utiliza un huésped creado con el comando **`virt-manager`**, ejecutando una instalación de Fedora totalmente virtualizada con una imagen ubicada en **`/var/lib/libvirt/images/Fedora.img`**. En este ejemplo se utiliza unl hipervisor Xen.

1. Cree el archivo de configuración XML para su imagen de huésped mediante el comando **`virsh`** en un huésped en ejecución.

   ```
   # virsh dumpxml Fedora > rhel5FV.xml
   ```

Esto guarda los parámetros de configuración en un archivo XML que puede ser editado para personalizar las operaciones y dispositivos utilizados por el huésped. Para obtener mayor información sobre el uso de XML de virsh, consulte *Capítulo 31, Creación de scripts libvirt personales*.

2. Cree una imagen de disquete para el huésped.

```
# dd if=/dev/zero of=/var/lib/libvirt/images/Fedora-floppy.img bs=512 count=2880
```

3. Añada el contenido a continuación, modificando lo que sea necesario, a su archivo de configuración XML de huésped'. Este ejemplo se trata de un dispositivo de disquete emulado utilizando una imagen basada en un archivo

```
<disk type='file' device='floppy'>
 <source file='/var/lib/libvirt/images/Fedora-floppy.img'/>
 <target dev='fda'/>
</disk>
```

4. Obligue al huésped a detenerse. Para apagar el huésped en una manera menos violenta, utilice en su lugar el comando **`virsh shutdown`**.

```
# virsh destroy Fedora
```

5. Detenga al huésped mediante el archivo de configuración XML.

```
# virsh create Fedora.xml
```

El dispositivo de disquete ahora está disponible en el huésped y está almacenado como un archivo de imagen en el anfitrión.

10.2. Cómo añadir dispositivos de almacenaje a huéspedes

Esta sección trata acerca de cómo agregarle dispositivos de almacenamiento a un huésped virtualizado. El almacenamiento adicional sólo puede agregarse después de la creación de huéspedes. Algunos de los dispositivos de almacenamiento y los protocoles compatibles son:

- particiones de discos duros locales,
- volúmenes lógicos,
- Canal de fibra o iSCSI conectado directamente al host.
- Contenedores de archivos que residen en un sistema de archivos en el host.
- Los sistemas de archivos **NFS** montados directamente por la máquina virtual.
- almacenamiento iSCSI accedido directamente por el huésped.
- Sistemas de archivos en clúster (**GFS**).

Cómo agregarle a un huésped almacenamientos basado en archivos

El archivo de almacenamiento o el archivo de contenedores son archivos en el sistema de archivos de huéspedes que actúan como discos duros para huéspedes virtualizados. Para agregar un contenedor de archivo realice los siguientes pasos:

1. Cree un archivo de contendor vacio o utilice un contendor de archivos ya existente (tal como un archivo ISO).

   a. Para crear un archivo disperso utilice el comando **dd**. Los archivos dispersos no se recomiendan, debido a que presentan problemas con la integridad de datos y el rendimiento. Estos archivos se crean mucho más rápido y pueden utilizarse para ensayar, pero no deben utilizarse en entornos de producción).

   ```
   # dd if=/dev/zero of=/var/lib/libvirt/images/FileName.img bs=1M seek=4096 count=0
   ```

   b. Se recomiendan archivos no-dispersos y pre-asignados para ser utilizados como imágenes de almacenamiento basadas en archivo. Para crear un archivo no-disperso, ejecute:

   ```
   # dd if=/dev/zero of=/var/lib/libvirt/images/FileName.img bs=1M count=4096
   ```

   Ambos comandos crean un archivo de 400MB que puede servir de almacenaje adicional para un huésped virtualizado.

2. Vacíe la configuración para el huésped. En este ejemplo el huésped se denomina *Guest1* y el archivo se guarda en el directorio principal de usuario.

   ```
   # virsh dumpxml Guest1 > ~/Guest1.xml
   ```

3. Abra el archivo de configuración (*Guest1.xml* en este ejemplo) en un editor de texto. Busque los elementos **<disk>**, ya que describen los dispositivos de almacenamiento. A continuación se observa un elemento de disco ejemplo:

   ```
   <disk type='file' device='disk'>
       <driver name='tap' type='aio'/>
       <source file='/var/lib/libvirt/images/Guest1.img'/>
       <target dev='xvda'/>
   </disk>
   ```

4. Añada el almacenamiento adicional duplicando o escribiendo un nuevo elemento **<disk>**. Asegúrese de heber especificado un nombre de dispositivo para los atributos del dispositivo de bloque virtual. Estos atributos deber ser diferentes para cada archivo de configuración de cada huésped. A continuación ofrecemos un ejemplo de una sección de un archivo de configuración que contiene un contenedor adicional de almacenamiento basado en un archivo, denominado **FileName.img**.

   ```
   <disk type='file' device='disk'>
       <driver name='tap' type='aio'/>
       <source file='/var/lib/libvirt/images/Guest1.img'/>
       <target dev='xvda'/>
   </disk>
   <disk type='file' device='disk'>
       <driver name='tap' type='aio'/>
       <source file='/var/lib/libvirt/images/FileName.img'/>
   ```

```
    <target dev='hda'/>
</disk>
```

5. Reinicie el huésped desde el archivo de configuración actualizado.

```
# virsh create Guest1.xml
```

6. Los siguientes pasos son específicos para el huésped de Linux. Otros sistemas operativos manejan los nuevos dispositivos de almacenamiento en formas diferentes. Para los sistemas que no sean Linux, consulte la documentación correspondiente a ellos.

   El huésped utiliza ahora el archivo **`FileName.img`** como el dispositivo llamado **`/dev/hdb`**. Este dispositivo requiere formato desde el huésped. En el huésped, divida el dispositivo en una partición primaria para todo el dispositivo luego de formato al dispositivo.

   a. Pulse *n* para una nueva partición.

   ```
   # fdisk /dev/hdb
   Comando (m for help):
   ```

   b. Pulse *p* para una partición primaria.

   ```
   Comando acción
      e   extendedida
      p   partición primaria (1-4)
   ```

   c. Elija el número de partición disponible. En este ejemplo la primera partición es seleccionada ingresando *1*.

   ```
   Partition number (1-4): 1
   ```

   d. Entre el primer cilindro predeterminado al pulsar *Enter*.

   ```
   Primer cilindro (1-400, predeterminado 1):
   ```

   e. Seleccione el tamaño de la partición. En este ejemplo todo el disco es asignado al pulsar la tecla *Enter*.

   ```
   Último cilindro o +tamaño o +tamañoM o +tamañoK (2-400, predeterminado 400):
   ```

   f. Establezca el tipo de partición al pulsar *t*.

   ```
   Command (m for help): t
   ```

   g. Elija la partición que ha creado en los pasos anteriores. En este ejemplo el número de la partición es *1*.

   ```
   Partition number (1-4): 1
   ```

   h. Ingrese *83* para una partición Linux.

```
Hex code (type L to list codes): 83
```

i. escriba los cambios al disco y salga.

```
Command (m for help): w
Command (m for help): q
```

j. De formato a la nueva partición con el sistema de archivos `ext3`.

```
# mke2fs -j /dev/hdb
```

7. Monte el disco en el huésped.

```
# mount /dev/hdb1 /myfiles
```

Ahora el huésped tiene un dispositivo de almacenamiento de archivo virtualizado adicional.

Cómo añadir discos duros y otros dispositivos de bloque a un huésped

Los administradores de sistemas utilizan discos duros adicionales para poder proporcionar más espacio de almacenamiento, o para poder mantener separados los datos del sistema y los datos del usuario. Este procedimiento, *Procedimiento 10.1, "Cómo añadir dispositivos de bloque físicos a huéspedes virtualizados."*, describe cómo añadir un disco duro en el equipo para un huésped virtualizado.

Los trabajos de procedimiento para todos los dispositivos de bloque físicos, incluye los CD-ROM, DVD y disquetes.

Seguridad en el dispositivo de bloque

El equipo no debería utilizar etiquetas de disco para identificar sistemas de archivo en los archivos **`fstab`** , **`initrd`**, o cualquier otro utilizado por la línea de comandos del kernel. Si se diera el caso que usuarios sin cierto nivel de autorización, especialmente huéspedes virtualizados, tengan acceso de escritura a particiones enteras, o volúmenes LVM, el sistema del equipo podría quedar comprometido

Los huéspedes no deberían tener acceso de escritura a discos enteros, o a dispositivos de bloques (por ejemplo, **`/dev/sdb`**). Los huéspedes virtualizados con acceso a dispositivos de bloques podrían ser capaces de acceder a otros dispositivos de bloques del sistema, o modificar etiquetas de volúmenes que pueden ser utilizadas para comprometer el sistema del equipo. Utilice particiones (por ejemplo, **`/dev/sdb1`**), o volúmenes LVM para prevenir estos inconvenientes.

Procedimiento 10.1. Cómo añadir dispositivos de bloque físicos a huéspedes virtualizados.

1. Conecte físicamente el dispositivo de disco duro al host. Configure el host si el controlador no es accesible por defecto.

2. Configure el dispositivo con **`multipath`** y se requiere persistencia en el host.

3. Utilice el comando **`virsh attach`**. Remplace: *`myguest`* por el nombre de su huésped, */dev/hdb1* por el dispositivo a añadir, y *hdc* por la ubicación para el dispositivo en el huésped. El *hdc* debe ser un nombre de dispositivo no utilizado. Utilice también la notación *hd** para huéspedes de Windows: el huésped reconocerá correctamente el dispositivo.

   Agregue el parámetro *`--type hdd`* al comando para dispositivos de CD-ROM o DVD.

   Agregue el parámetro *`--type floppy`* al comando para dispositivos de disquete.

```
# virsh attach-disk myguest
     /dev/hdb1
     hdc --driver tap --mode readonly
```

4. Ahora el huésped tiene un nuevo disco duro llamado **`/dev/hdb`** en Linux o **`D: drive`**, o similar, en Windows. Este dispositivo puede requerir formateo.

10.3. Cómo configurar almacenamiento persistente en Fedora

Esta sección es para sistemas con almacenamiento externo o de red; es decir, Fibre Channel o dispositivos de almacenaje iSCSI. Se recomienda que dichos sistemas tengan nombres de dispositivos persistentes configurados para sus hosts. Así se ayuda a la migración en vivo como también a proporcionar nombres de dispositivos consistentes y almacenaje para sistemas virtualizados múltiples.

Los identificadores únicos universales o UUID (Universally Unique Identifiers) son un método estandarizado para la identificación de computadores y dispositivos en entornos informáticos de distribución. Esta sección utiliza los UUID para identificar a iSCSI o LUN de Fibre Channel. Los UUID persisten después del reinicio, desconexión e intercambio de dispositivos. El UUID es similar a una etiqueta en el dispositivo.

Los sistemas que no estén ejecutando **`multipath`**, deben utilizar*Configuración de ruta única*. Los sistemas que estén ejecutando **`multipath`**, pueden utilizar *Configuración de multi-rutas*.

Configuración de ruta única

Este procedimiento implementa la persisitencia de dispositivo *LUN* mediante **`udev`**. Sólo utilice este procedimiento para equipos que no estén utilizando **`multipath`**.

1. Edite el archivo **`/etc/scsi_id.config`**.

   - Añada la siguiente línea:

     ```
     opciones=--whitelisted --replace-whitespace
     ```

     Esto define las opciones predeterminadas para scsi_id, asegurando que los UUIDs obtenidos no contengan espacios. De lo contratio, el destino IET iSCSI devuelve espacios en los UUIDs, lo que puede generar problemas.

2. Para conocer el UUID de un dispositivo determinado, ejecute el comando **`scsi_id --whitelisted --replace-whitespace --device=/dev/sd*`**. Por ejemplo:

```
# scsi_id --whitelisted --replace-whitespace --device=/dev/sdc
```

```
1IET_00010001
```

El resultado puede ser diferente que el ejemplo anterior. En nuestro ejemplo, la salida presenta el UUID del dispositivo `/dev/sdc`.

3. Verifique que la salida de UUID mediante el comando **`scsi_id --whitelisted --replace-whitespace --device=/dev/sd*`** sea correcta y coherente.

4. Cree una regla para nombrar el dispositivo. Cree un archivo llamado **`20-names.rules`** en el directorio **`/etc/udev/rules.d`**. Añada nuevas reglas a este archivo. Todas las reglas se añaden al mismo archivo utilizando el mismo formato. Las reglas siguen el siguiente formato:

```
KERNEL=="sd*", SUBSYSTEM=="block", PROGRAM="/sbin/scsi_id --whitelisted --replace-
whitespace /dev/$name", RESULT=="UUID", NAME="devicename"
```

Remplace *`UUID`* y *`devicename`* por el UUID recibido anteriormente y el nombre dado para el dispositivo. El siguiente es un ejemplo para la regla anterior:

```
KERNEL=="sd*", SUBSYSTEM=="block", PROGRAM="/sbin/scsi_id --whitelisted --replace-
whitespace /dev/$name", RESULT=="1IET_00010001", NAME="rack4row16lun1"
```

El demonio **`udev`** ahora busca todos los dispositivos denominados **`/dev/sd*`** para el UUID en la regla. Una vez que el dispositivo coincidente esté conectado al sistema, se le asignará un nombre desde la regla. En el ejemplo anterior, un dispositivo con un UUID de 1IET_00010001 aparecería como **`/dev/rack4row16lun1`**.

5. Copie en todos los equipos relevantes las modificaciones en los archivos **`/etc/scsi_id.config`** y **`/etc/udev/rules.d/20-names.rules`** .

Los dispositivos de almacenamiento de red con reglas configuradas ahora tienen nombres persistentes en todos los hosts donde los archivos han sido actualizados. Esto significa que puede migrar huéspedes entre hosts mediante el almacenamiento compartido y los huéspedes pueden acceder a los dispositivos de almacenaje en sus archivos de configuración.

Configuración de multi-rutas

El paquete **`multipath`** es utilizado para sistemas que posean más de una ruta física desde el computador hacia los dispositivos de almacenamiento. **`multipath`** ofrece tolerancia a fallos, recuperación de fallos y rendimiento mejorado para dispositivos de almacenamiento de red asociados a sistemas fedora.

Para poder implementar persistencia Lun en un entorno **`multipath`**, debe definir los sobrenombres de sus dispositivos multipath. Cada dispositivo de almacenamiento posee un UUID que actúa como una llave para los sobrenombres. Identifique un UUID de dispositivo mediante el comando **`scsi_id`**.

```
# scsi_id --whitelisted --replace-whitespace --device=/dev/sdc
```

Los dispositivos multipath serán creados en el directorio **`/dev/mpath`**. En el ejemplo a continuación 4 dispositivos están definidos en **`/etc/multipath.conf`**:

```
multipaths {
 multipath {
 wwid  3600805f30015987000000000768a0019
 alias  oramp1
```

```
 }
 multipath {
 wwid  3600805f30015987000000000d643001a
 alias  oramp2
 }
 mulitpath {
 wwid  3600805f3001598700000000086fc001b
 alias  oramp3
 }
 mulitpath {
 wwid  3600805f300159870000000000984001c
 alias  oramp4
 }
}
```

Esta configuración creará 4 LUNs denominados **/dev/mpath/oramp1**, **/dev/mpath/oramp2**, **/dev/mpath/oramp3** y **/dev/mpath/oramp4**. Una vez introducidos, el mapeo de los WWID de dispositivos a sus nuevos nombres será persistente luego del reinicio.

10.4. Cómo añadir dispositivos CD-ROM o DVD a un huésped

Para asociar un archivo ISO a un huésped mientras el huésped se encuentre en línea, utilice el comando **virsh** con el parámetro *attach-disk*.

```
# virsh attach-disk [domain-id] [source] [target] --driver file --type cdrom --mode readonly
```

Los parámetros *source* y *target* son rutas para los archivos y dispositivos, en el equipo y en el huésped respectivamente. El parámetro *source* puede ser una ruta para un archivo ISO o el dispositivo desde el directorio **/dev**.

Configuración de la red

Esta página proporciona una introducción a las configuraciones de red más comunes utilizadas por las aplicaciones basadas en libvirt. Para obtener información adicional, consulte los documentos de arquitectura de red de libvirt.

The two common setups are "virtual network" or "shared physical device". The former is identical across all distributions and available out-of-the-box. The latter needs distribution specific manual configuration.

De manera predeterminada, los serivicios de red de los huéspedes virtualizados no son accesibles desde equipos externos. Debe habilitarse o bien NAT (Network adress trannslation), o bien un puente de Red para permitir que los equipos externos puedan acceder a los servicios de red de los huéspedes virtualizados.

11.1. Traducción de dirección de red (NAT) con libvirt

Uno de los métodos más comunes para compartir conexiones de red es utilizar el reenvío de la traducción de dirección de red (NAT) (también conocida como redes virtuales).

Configuración de host

Every standard `libvirt` installation provides NAT based connectivity to virtual machines out of the box. This is the so called 'default virtual network'. Verify that it is available with the **`virsh net-list --all`** command.

```
# virsh net-list --all
Name                 State      Autostart
-----------------------------------------
default              active     yes
```

Si no está disponible, el archivo de configuración XML de ejemplo se puede volver a cargar y activar:

```
# virsh net-define /usr/share/libvirt/networks/default.xml
```

La red predeterminada está definida desde **`/usr/share/libvirt/networks/default.xml`**

Señale la red predeterminada para iniciar automáticamente:

```
# virsh net-autostart default
Network default marked as autostarted
```

Iniciar la red predeterminada:

```
# virsh net-start default
Network default started
```

Una vez la red predeterminada de `libvirt` está en ejecución, se podrá ver un dispositivo de puente aislado. Este dispositivo *no* tiene interferencias físicas agregadas desde que utiliza NAT y reenvío IP para conectarse fuera del mundo. No añada nuevas interfaces.

```
# brctl show
```

```
bridge name     bridge id               STP enabled     interfaces
virbr0          8000.000000000000       yes
```

libvirt añade reglas **iptables** que permiten el tráfico hacia y desde huéspedes añadidos al dispositivo `virbr0` en las cadenas **INPUT**, **FORWARD**, **OUTPUT** y **POSTROUTING**. Luego, **libvirt** intenta activar el parámetro **ip_forward**. Otras aplicaciones pueden desactivar **ip_forward**, por eso la mejor opción es añadir lo siguiente a **/etc/sysctl.conf**.

```
net.ipv4.ip_forward = 1
```

Configuración del huésped

Once the host configuration is complete, a guest can be connected to the virtual network based on its name. To connect a guest to the 'default' virtual network, the following XML can be used in the guest:

```
<interface type='network'>
  <source network='default'/>
</interface>
```

Nota

Definir una dirección MAC es opcional. La dirección MAC se genera automáticamente si se omite. Establecer la dirección MAC en forma manual es útil en algunas situaciones.

```
<interface type='network'>
  <source network='default'/>
  <mac address='00:16:3e:1a:b3:4a'/>
  </interface>
```

11.2. Creación de redes en puente con libvirt

La creación de redes en puente (también conocido como compartir dispositivos físicos) sirve para dedicar un dispositivo físico a una máquina virtual. El puente se utiliza para configuraciones más avanzadas y en servidores con múltiples interfaces de red.

Inhabilitar el NetworkManager

NetworkManager no soporta puentes. NetworkManager debe estar deshabilitado para poder utilizar la red, con los programas de red (ubicados en el directorio **/etc/sysconfig/network-scripts/**).

```
# chkconfig NetworkManager off
# chkconfig network on
# service NetworkManager stop
# service network start
```

Nota

Instead of turning off **NetworkManager**, add "*NM_CONTROLLED=no*" to the **ifcfg-*** scripts used in the examples.

Creación de initscripts de redes

Cree o edite los siguientes dos archivos de configuración de redes. Este paso puede repetirse (con nombres diferentes) para puentes de red adicionales.

Cambie al directorio **`/etc/sysconfig/network-scripts`**:

```
# cd /etc/sysconfig/network-scripts
```

Abra el script de redes para el dispositivo que usted está añadiendo al puente. En este ejemplo, **`ifcfg-eth0`** define la interfaz de red física establecida como parte de un puente:

```
DEVICE=eth0
# change the hardware address to match the hardware address your NIC uses
HWADDR=00:16:76:D6:C9:45
ONBOOT=yes
BRIDGE=br0
```

Consejo

You can configure the device's Maximum Transfer Unit (MTU) by appending an *`MTU`* variable to the end of the configuration file.

```
MTU=9000
```

Cree un nuevo script de red en el directorio **`/etc/sysconfig/network-scripts`** llamado **`ifcfg-br0`** o parecido. El parámetro *`br0`* es el nombre del puente, éste puede ser cualquier cosa, siempre y cuando el nombre del archivo sea el mismo del parámetro de DEVICE.

```
DEVICE=br0
TYPE=Bridge
BOOTPROTO=dhcp
ONBOOT=yes
DELAY=0
```

Advertencia

The line, *`TYPE=Bridge`*, is case-sensitive. It must have uppercase 'B' and lower case 'ridge'.

Tras la configuración, reinicie la creación de redes o reinicie.

```
# service network restart
```

Configure **`iptables`** para permitir que todo el tráfico sea reenviado a través del puente.

```
# iptables -I FORWARD -m physdev --physdev-is-bridged -j ACCEPT
# service iptables save
# service iptables restart
```

Deshabilite iptables en los puentes

De forma alternativa, evite que el tráfico de los puentes sea procesado por las reglas de **iptables**. Agregue las líneas siguientes en el archivo **/etc/sysctl.conf**:

```
net.bridge.bridge-nf-call-ip6tables = 0
net.bridge.bridge-nf-call-iptables = 0
net.bridge.bridge-nf-call-arptables = 0
```

Vuelva a cargar los parámetros del kernel configurados com el comando **sysctl**.

```
# sysctl -p /etc/sysctl.conf
```

Reinicie el demonio de **libvirt**

```
# service libvirtd reload
```

You should now have a "shared physical device", which guests can be attached and have full LAN access. Verify your new bridge:

```
# brctl show
bridge name     bridge id               STP enabled     interfaces
virbr0          8000.000000000000       yes
br0             8000.000e0cb30550       no              eth0
```

Observe que, el puente esté completamente independiente del puente **virbr0**. *No* intente conectar el dispositivo físico a **virbr0**. El puente **virbr0** es únicamente para conectividad de Traducción de dirección de redes (NAT).

Controladores KVM para-virtualizados

Los controladores para-virtualizados están disponibles para huéspedes de Windows ejecutándose en hosts KVM. Estos controladores para-virtualizados se incluyen en el paquete de virtualización. El paquete Virtio soporta dispositivos de almacenamento (bloque) y controladores de interfaz de red.

Los controladores para-virtualizados aumentan el rendimiento de los huéspedes totalmente para-virtualizados. Con los controladores para-virtualizados la latencia de E/S disminuye y el rendimiento aumenta los niveles a casi bare- metal. Es recomendable utilizar controladores para-virtualizados para huéspedes completamente virtualizados ejecutando tareas pesadas de E/S y aplicaciones.

Los controladores para-virtualizados son cargados automáticamente, y son instalados en:

- Cualquier kernel 2.6.27 o superior.
- Nuevos Ubuntu, CentOS, Linux para empresas de Red Hat.

Esas versiones de Linux detectan e instalan los controladores para que no sean necesarios pasos de instalación adicionales.

Nota

Los dispositivos PCI están limitados por la arquitectura del sistema virtualizado. De los 32 dispositivos disponibles para un huésped, 2 no son removibles. Esto significa que existen 30 slots PCI disponibles por huésped para dispositivos adicionales. Cada dispositivo PCI puede realizar hasta 8 funciones; algunos posee múltiples funciones y sólo utilizan un slot. Utilizan slots o funciones una red para-virtualizada, dispositivos de discos para-virtualizados, o cualquier otro dispositivo PCI que utilice VT-d. El número exacto de dispositivos disponibles es difícil de calcular debido a su gran cantidad. Cada huésped puede utilizar hasta 32 dispositivos PCI, y cada uno de ellos siendo capaz de realizar hasta 8 funciones.

Las siguientes versiones de Microsoft Windows deberían poseer controladores para-virtualizados KVM que funcionen:

- Windows XP (solo 32 bits)
- Windows Server 2003 (versiones de 32 y de 64 bits)
- Windows Server 2008 (versiones de 32 y de 64 bits)
- Windows 7 (versiones de 32 y de 64 bits)

12.1. Instalacion de controladores KVM Windows para-virtualizados

Esta sección cubre el proceso de instalación para los controladores KVM Windows para-virtualizados. Los controladores KVM para-virtualizados pueden ser cargados durante la instalación de Windows o después de la instalación del huésped.

Puede instalar los controladores para-virtualizados de su huésped con alguno de los métodos siguientes:

- almacenando los archivos de instalación en una red accesible al huésped,
- Utilizando un dispositivo de CD-ROM virtualizado del archivo .iso del controlador de instalación, o
- utilizando un dispositivo de disquette para instalar los controladores durante el momento del arranque (para huéspedes Windows).

Esta guía describe la instalación desde el disco instalador para-virtualizado, como un dispositivo de CD-ROM virtualizado.

1. **Descargar los controladores**
   El paquete *virtio-win* contiene el bloque para-virtualizado y los controladores de red para todos los huéspedes Windows que deberían ser capaces de funcionar.

   Descargue el paquete *virtio-win* mediante el comando **yum**.

   ```
   # yum install virtio-win
   ```

   Los controladores son también para Microsoft (*windowsservercatalog.com*[1]).

   El paquete *virtio-win* instala una imagen de CD-ROM (el archivo **virtio-win.iso**) en el directorio **/usr/share/virtio-win/**.

2. **Instale los controladores para-virtualizados**
   Se recomienda instalar los controladores en el huésped antes de anexar o modificar un dispositivo para usar los controladores para-virtualizados.

   Para dispositivos de bloque que almacenan sistemas de archivos de root u otros dispositivos de bloque requeridos para arrancar el húesped, los controladores deben ser instalados antes que el dispositivo sea modificado. Si los controladores no están instalados en el huésped y el controlador está configurado para el controlador de virtio, el huésped no podrá arrancar.

Cómo instalar los controladores con un CD-ROM virtualizado

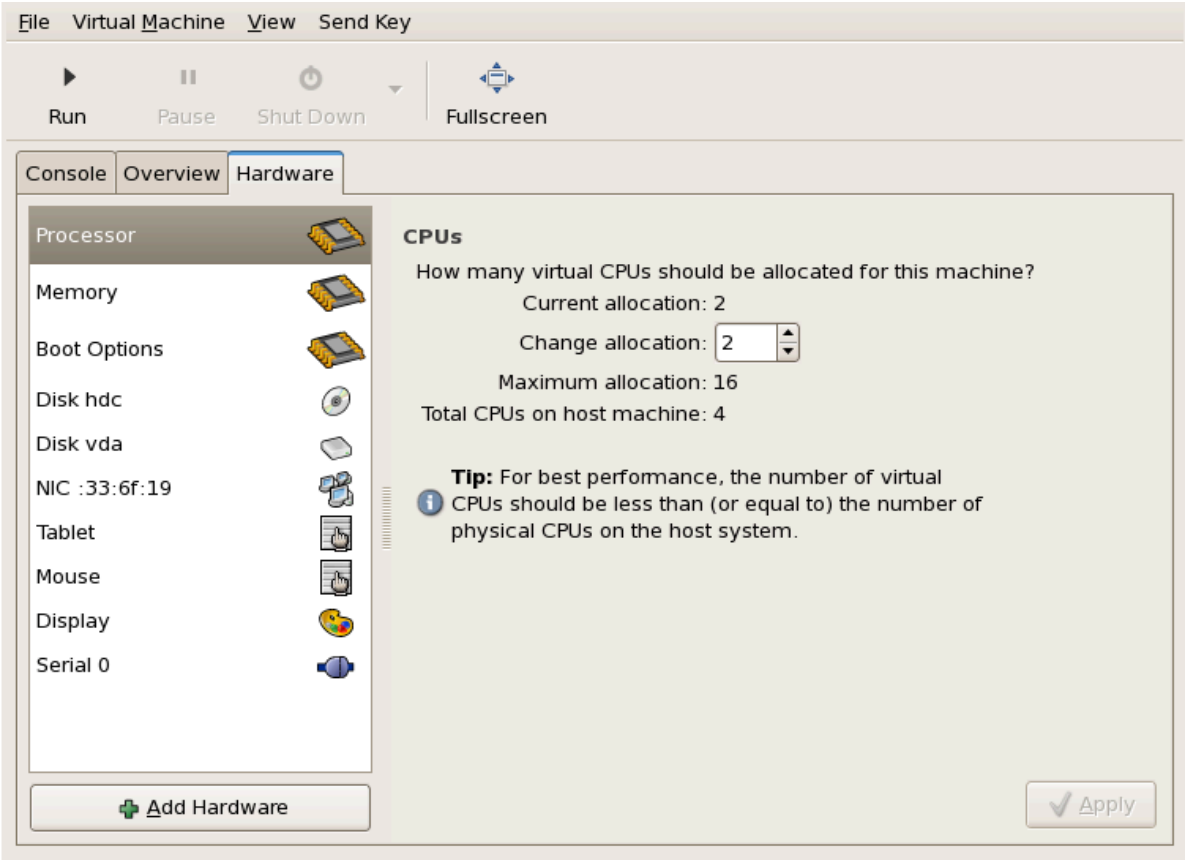
Este procedimiento describe la instalación de controladores para-virtualizados con un CD-ROM virtualizado, luego que Windows haya sido instalado.

Consulte, *Procedimiento 12.1, "Uso de **virt-manager** para montar una imagen de CD-ROM para un huésped de a Windows"* para agregar una imagen de CD-ROM con **virt-manager**, y luego instalar los controladores.

Procedimiento 12.1. Uso de **virt-manager** para montar una imagen de CD-ROM para un huésped de a Windows

1. **Inicie virt-manager y el huésped virtualizado**
   Abra **virt-manager**, seleccione su huésped virtualizado desde la lista haciendo doble clic sobre el nombre del huésped.

2. **Abrir la pestaña de Hardware**
   Haga clic en el botón **Agregar hardware** en la pestaña de **Hardware**.



3. **Seleccione el tipo de dispositivo**
   Esto inicia un asistente para agregar el nuevo dispositivo. Seleccione **Almacenamiento** desde el menú desplegable.

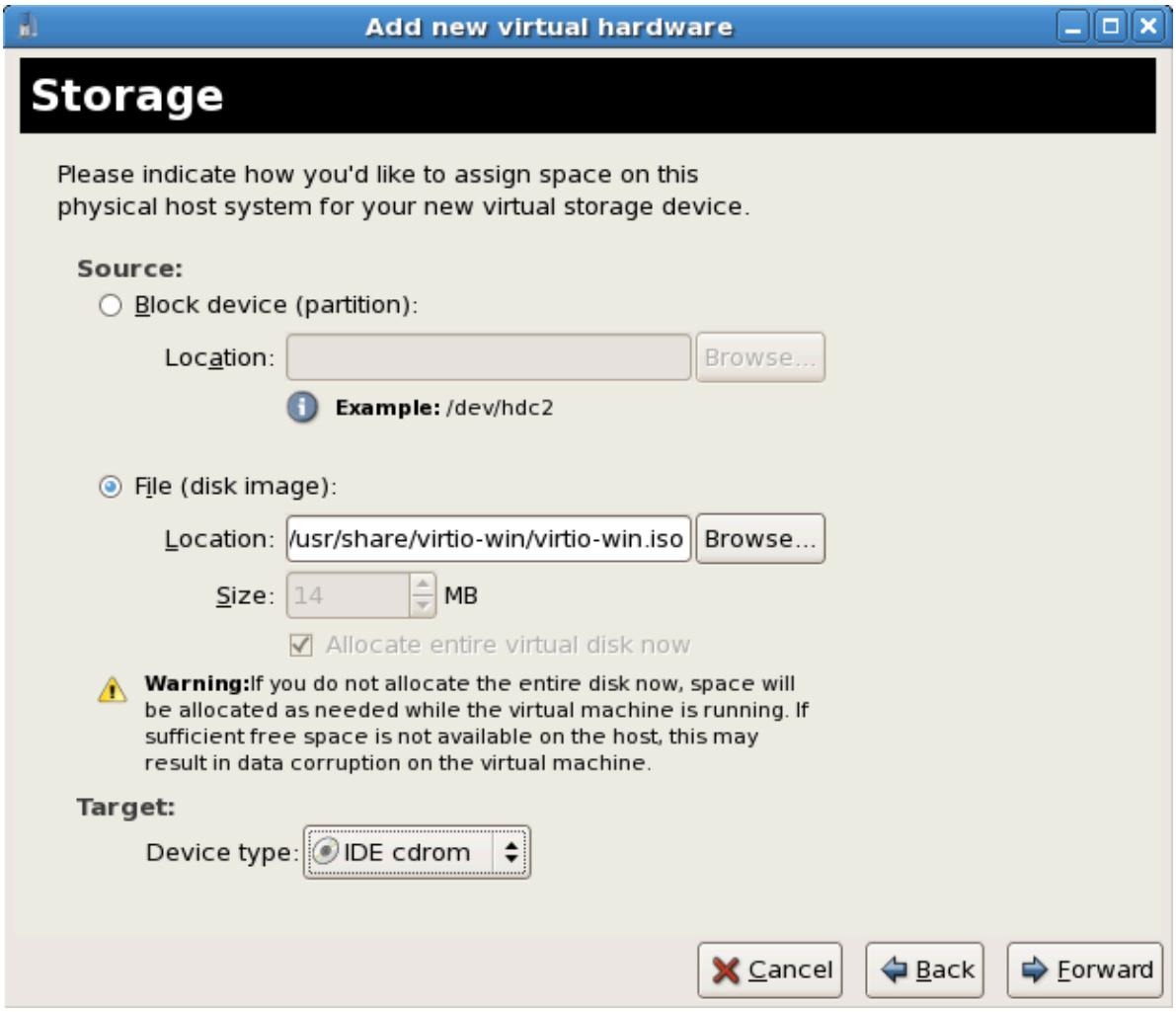
Add new virtual hardware
Adding new virtual hardware
This assistant will guide you through adding a new piece of virtual hardware. First select what type of hardware you wish to add:
Hardware type:
Storage device
Cancel
Back
Forward

Haga clic sobre el botón **Avanzar** para continuar.

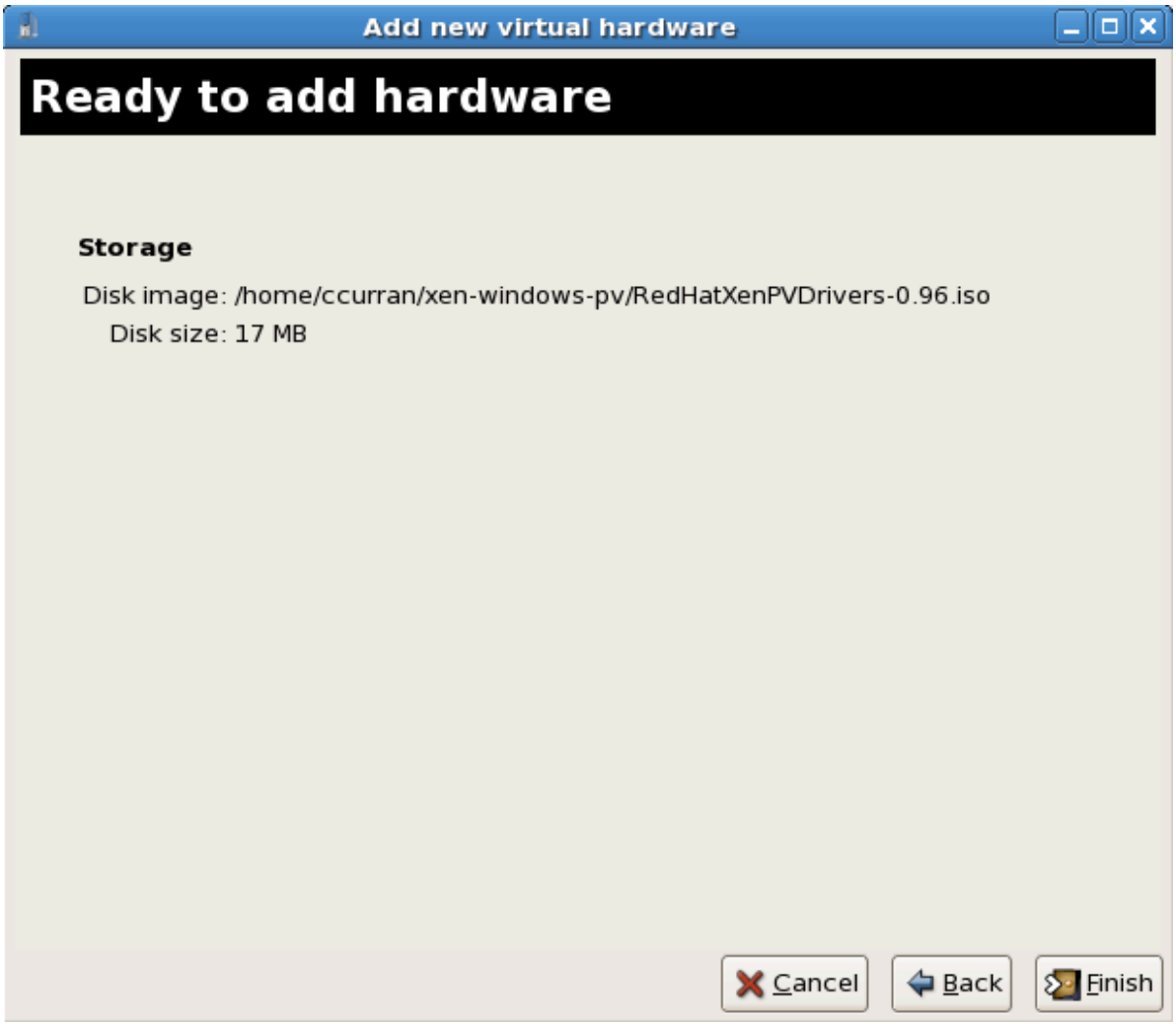
4. **Seleccione el archivo ISO**
   Elija la opción **Archivo (imagen de disco)** y defina la ubicación del archivo .iso de los controladores para-virutalizados. La ubicación de los archivos es denominada **`/usr/share/virtio-win/virtio-win.iso`**.

   Si los controladores se encuentran almacenados en CD físicos, utilice la opción **Normal Disk Partition**.

   Defina el **Tipo de dispositivo** para **IDE cdrom** y haga clic en **Adelante** para proseguir.


Add new virtual hardware
Storage
Please indicate how you'd like to assign space on this physical host system for your new virtual storage device.
Source:
Block device (partition):
Location:
Browse...
Example: /dev/hdc2
File (disk image):
Location: /usr/share/virtio-win/virtio-win.iso
Browse...
Size: 14 MB
Allocate entire virtual disk now
Warning: If you do not allocate the entire disk now, space will be allocated as needed while the virtual machine is running. If sufficient free space is not available on the host, this may result in data corruption on the virtual machine.
Target:
Device type: IDE cdrom
Cancel
Back
Forward

5. **Disco asignadoi**
   El disco ha sido asignado y se encuentra disponible para el huésped una vez que éste sea iniciado. Haga clic en **Finalizar** para cerrar el asistente o "regresar", si ha cometido algún error.

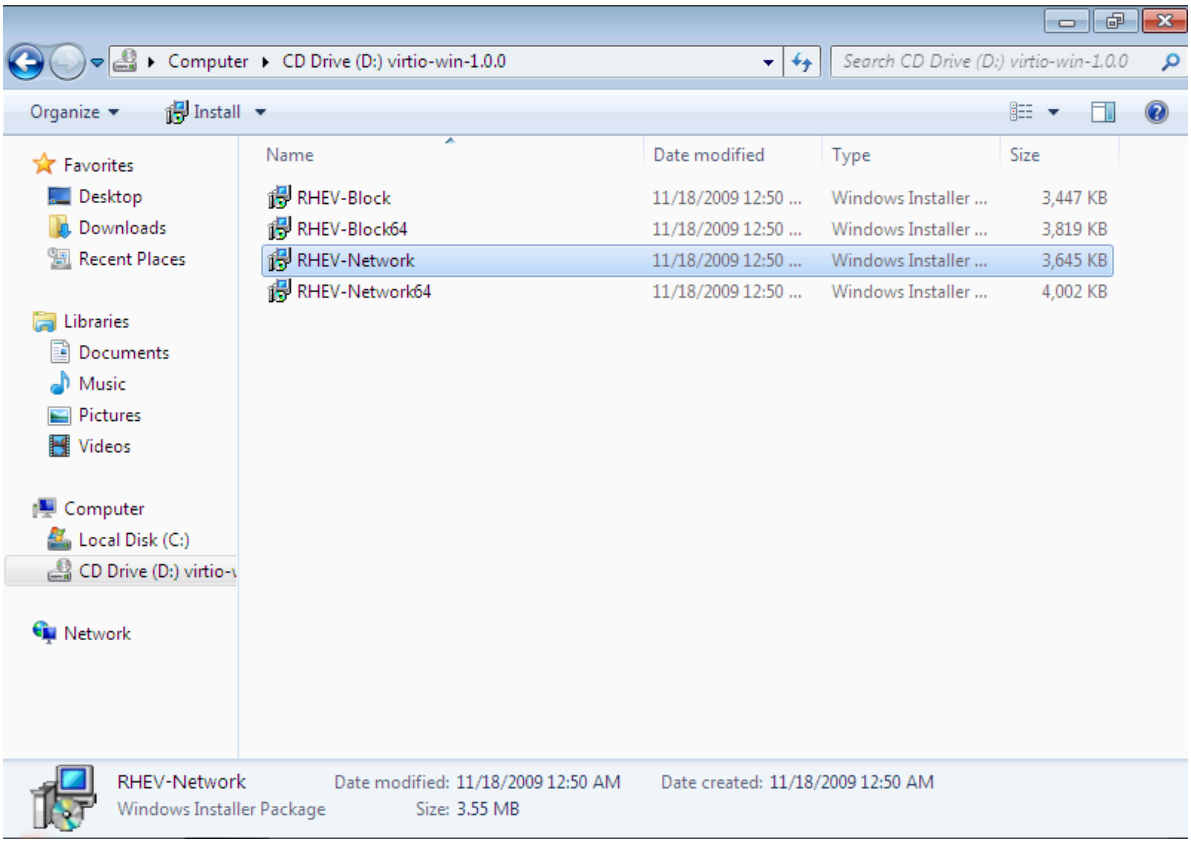


6. **Reinicie**
   Reinicie o inicie el huésped para agregar el nuevo dispositivo. Los dispositivos virtualizados IDE necesitan reiniciarse antes de que puedan ser reconocidos por los huéspedes

Una vez sea asociado el CD-ROM con los controladores, y que el huésped haya sido iniciado, proceda con *Procedimiento 12.2, "Instalación de Windows"*.

Procedimiento 12.2. Instalación de Windows

1. **Abra Mi PC**
   En el huésped Windows, abra **Mi PC** y elija el dispositivo CD-ROM.

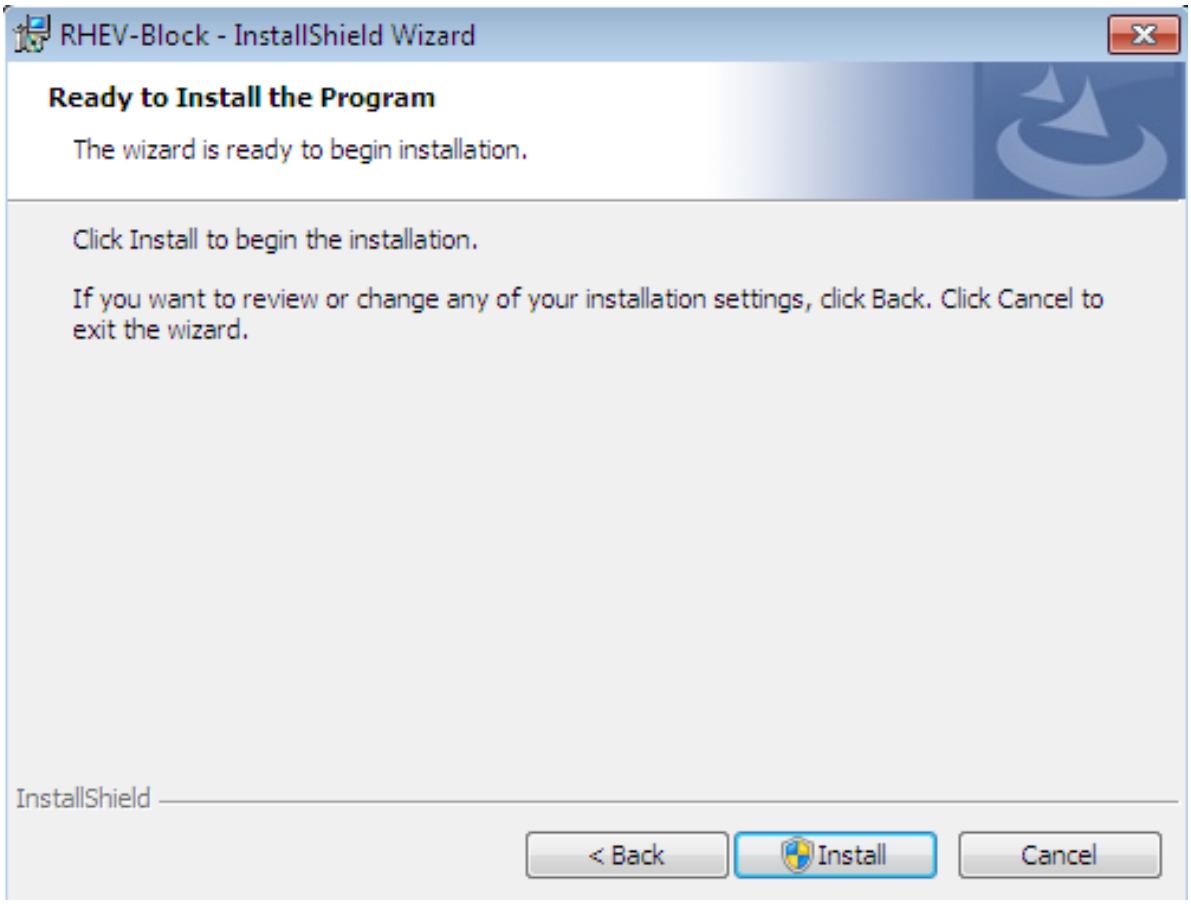


2. **Elija los archivos de instalación correctos**
   There are four files available on the disc. Select the drivers you require for your guest's architecture:

   - el controlador de dispositivo de bloque para-virtualizado (**`RHEV-Block.msi`** para huéspedes de 32 bits, o **`RHEV-Block64.msi`** para huéspedes de 64 bits),
   - el controlador de dispositivo de red para-virtualizado (**`RHEV-Network.msi`** para huéspedes de 32 bits, o **`RHEV-Network64.msi`** para huéspedes de 64 bits),
   - o ambos controladores de dispositivos: el de red y el de bloques.

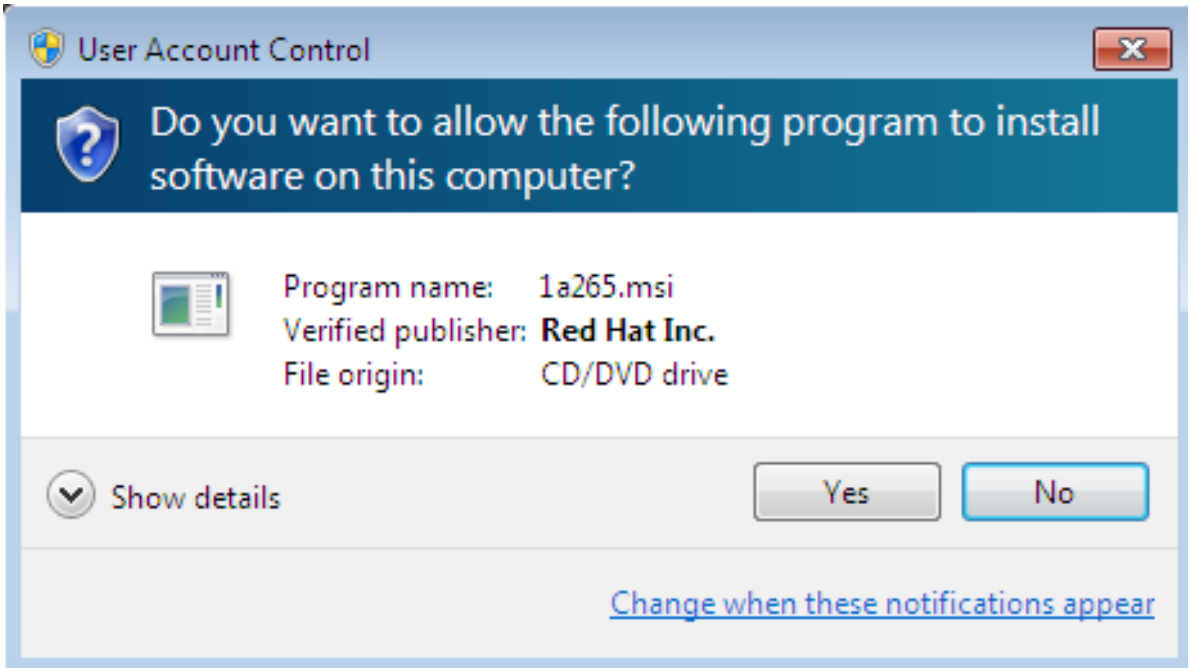
   Haga un doble clic sobre los archivos de instalación para instalar los controladores.

3. **Instale el controlador de dispositivos de bloque**
   a. **Inicie la instalación del controlador de dispositivos de bloques**
      Haga un doble clic en **`RHEV-Block.msi`** o en **`RHEV-Block64.msi`**.


RHEV-Block - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

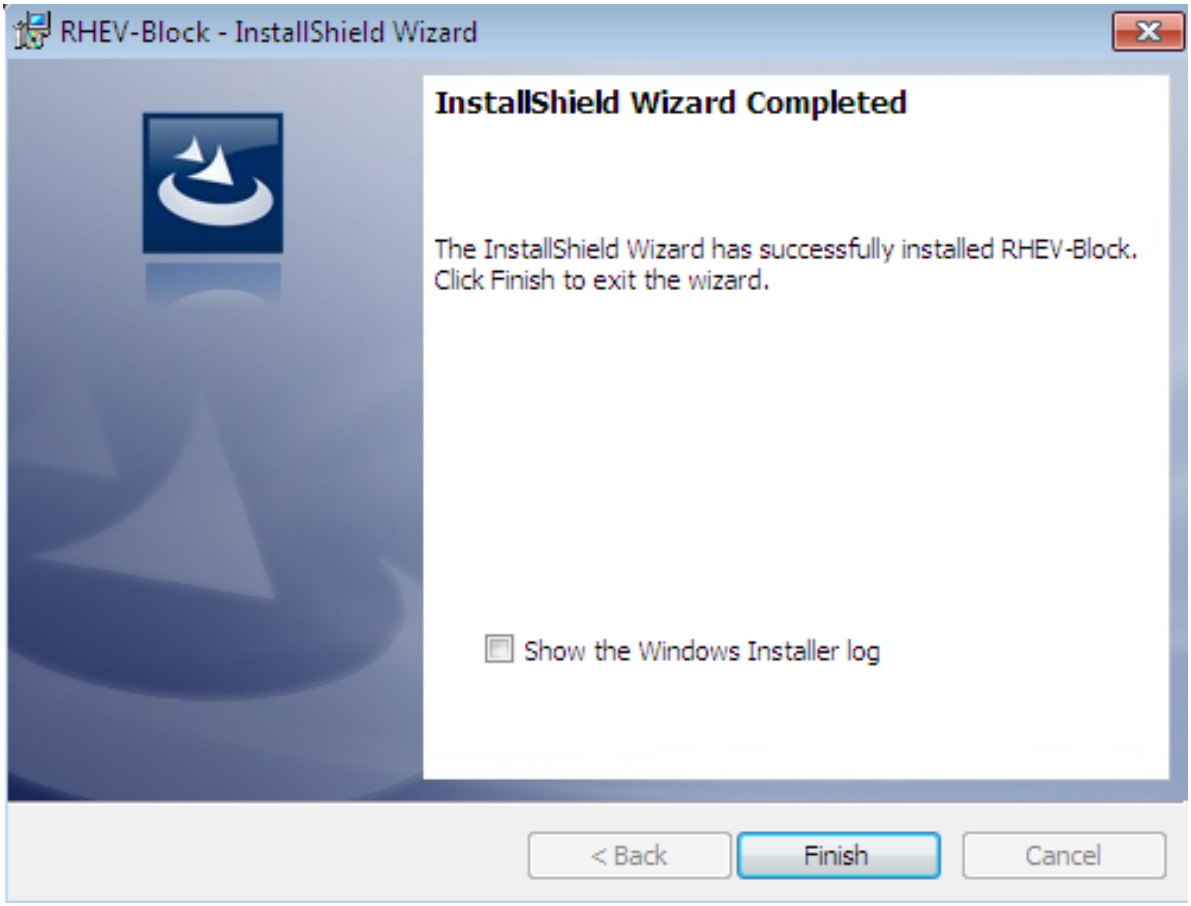
Presione el botón **Next** para continuar.

b. **Confirme la excepción**
Windows podría preguntarle por una excepción de seguridad.


User Account Control
Do you want to allow the following program to install software on this computer?
Program name: 1a265.msi
Verified publisher: Red Hat Inc.
File origin: CD/DVD drive
Show details
Yes
No
Change when these notifications appear

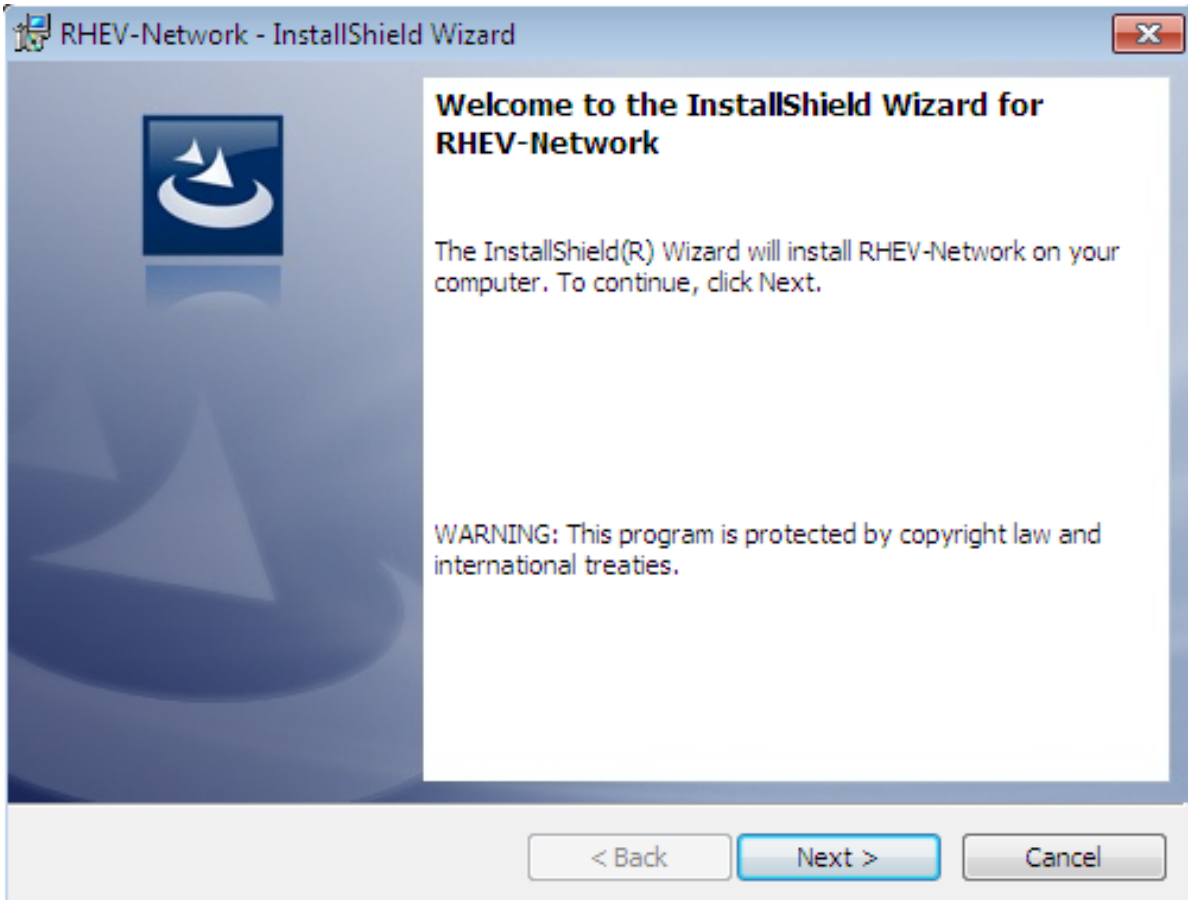
Presione **Yes** si es correcto.

c. **Finalizar**


RHEV-Block - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed RHEV-Block. Click Finish to exit the wizard.
Show the Windows Installer log
< Back
Finish
Cancel

Presione **Finalizar** para completar la instalación.

4. **Instale el controlador de dispositivos de red**
   a. **Inicie la instalación del controlador del dispositivo de red**
   Haga doble clic sobre **`RHEV-Network.msi`**, o sobre **`RHEV-Network64.msi`**.


RHEV-Network - InstallShield Wizard
Welcome to the InstallShield Wizard for RHEV-Network
The InstallShield(R) Wizard will install RHEV-Network on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

Presione el botón **Next** para continuar.

b. **Configuración del desempeño**

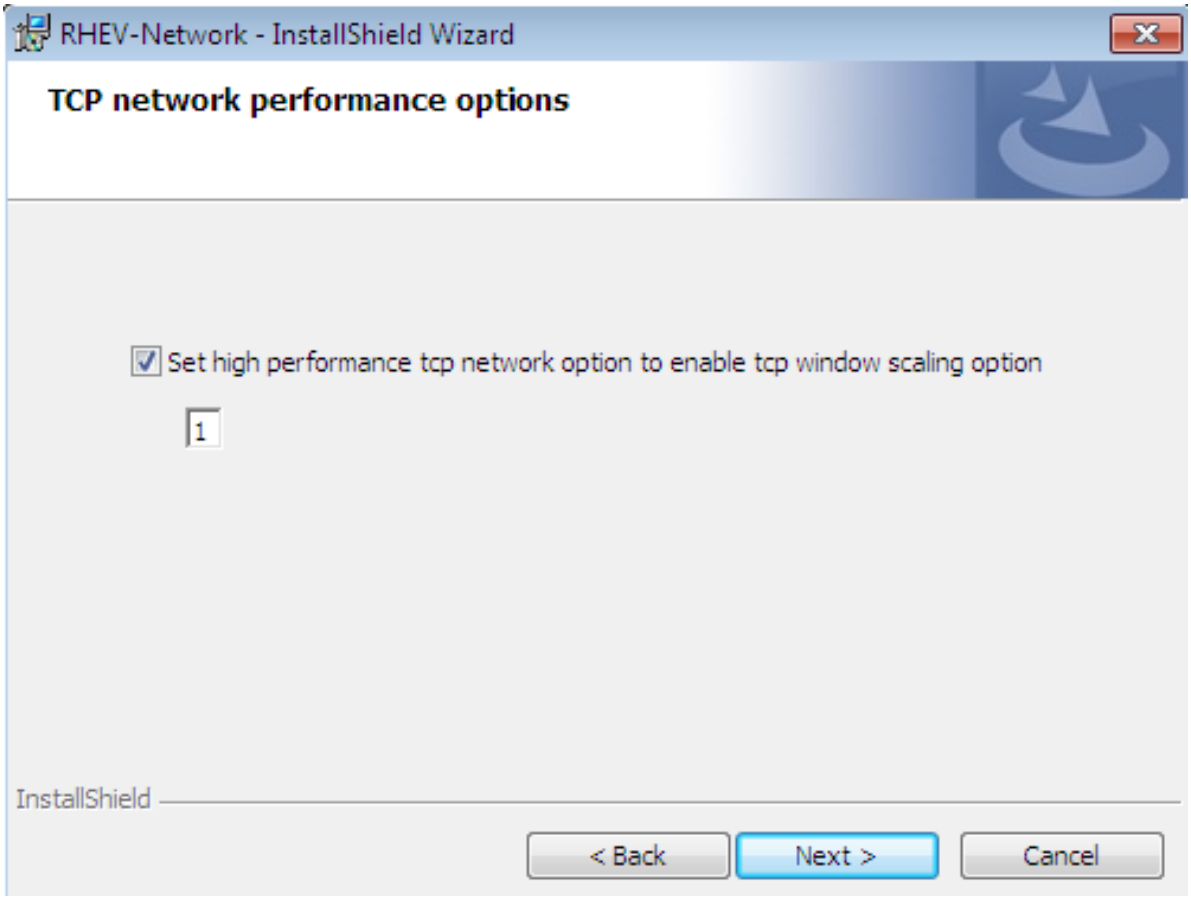
En esta pantalla se realizan configuraciones TCP avanzadas para el controlador de red. Las marcas de tiempo y el escalado de la ventana son opciones que pueden ser habilitadas o deshabilitadas. El valor predeterminado para que el escalado de ventanas esté activado es 1.

El escalado de ventanas TCP se describe con más detalle en *IETF RFC 1323*[2]. La RFC define un método para aumentar la recepción del tamaño de la ventana (por defecto permitido a 65.535 bytes), hasta un máximo de 1 gigabyte (1,073,741,824 bytes). El escalado de ventanas TCP permite a las redes transferir datos con niveles muy cercanos a los límites teóricos del ancho de banda. Ventanas de recepción mayores podrían no funcionar correctamente con determinado hardware de red, o sistemas operativos.

Las marcas de tiempo TCP son también definidas en *IETF RFC 1323*[3]. Son utilizadas para calcular mejor el tiempo de viaje de regreso estimado por la información de sincronización contenida en paquetes incrustados. Las marcas de tiempo TCP ayudan al sistema a adaptarse a los inestables niveles de tráfico, y evitar problemas de congestión en redes muy concurridas.

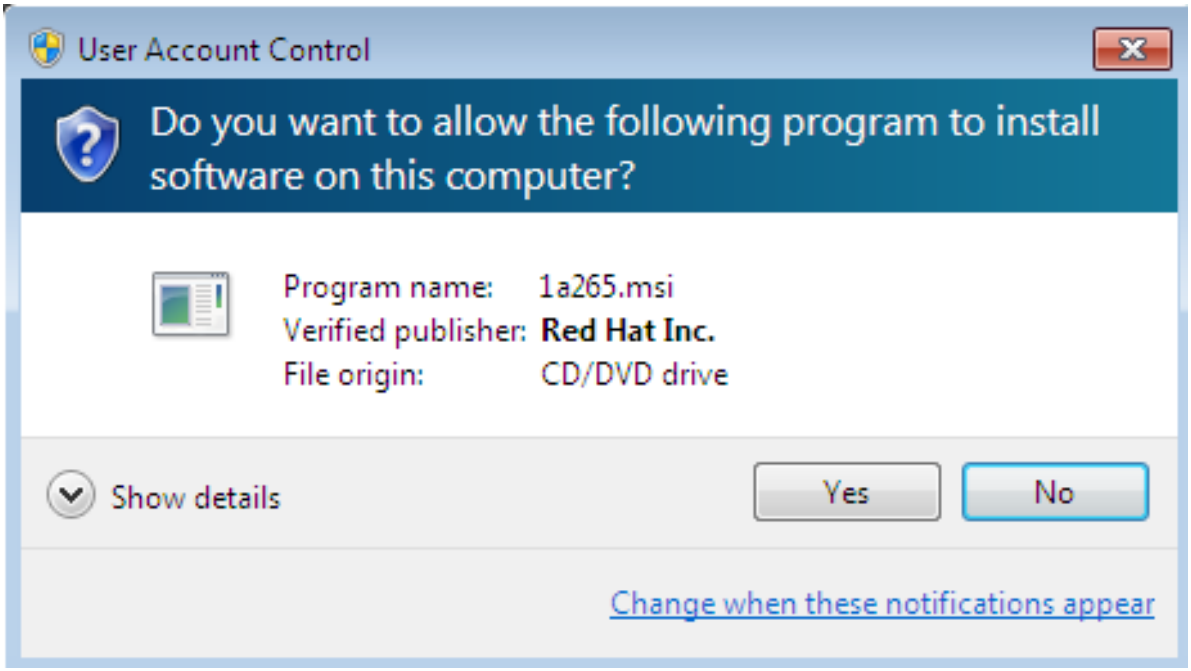
Valor	Acción
0	Deshabilita marcas de tiempo TCP y escalado de ventanas.

Valor	Acción
1	Habilita escalado de ventanas TCP.
2	Habilita marcas de tiempo TCP.
3	Habilita marcas de tiempo TCP y escalado de ventanas.



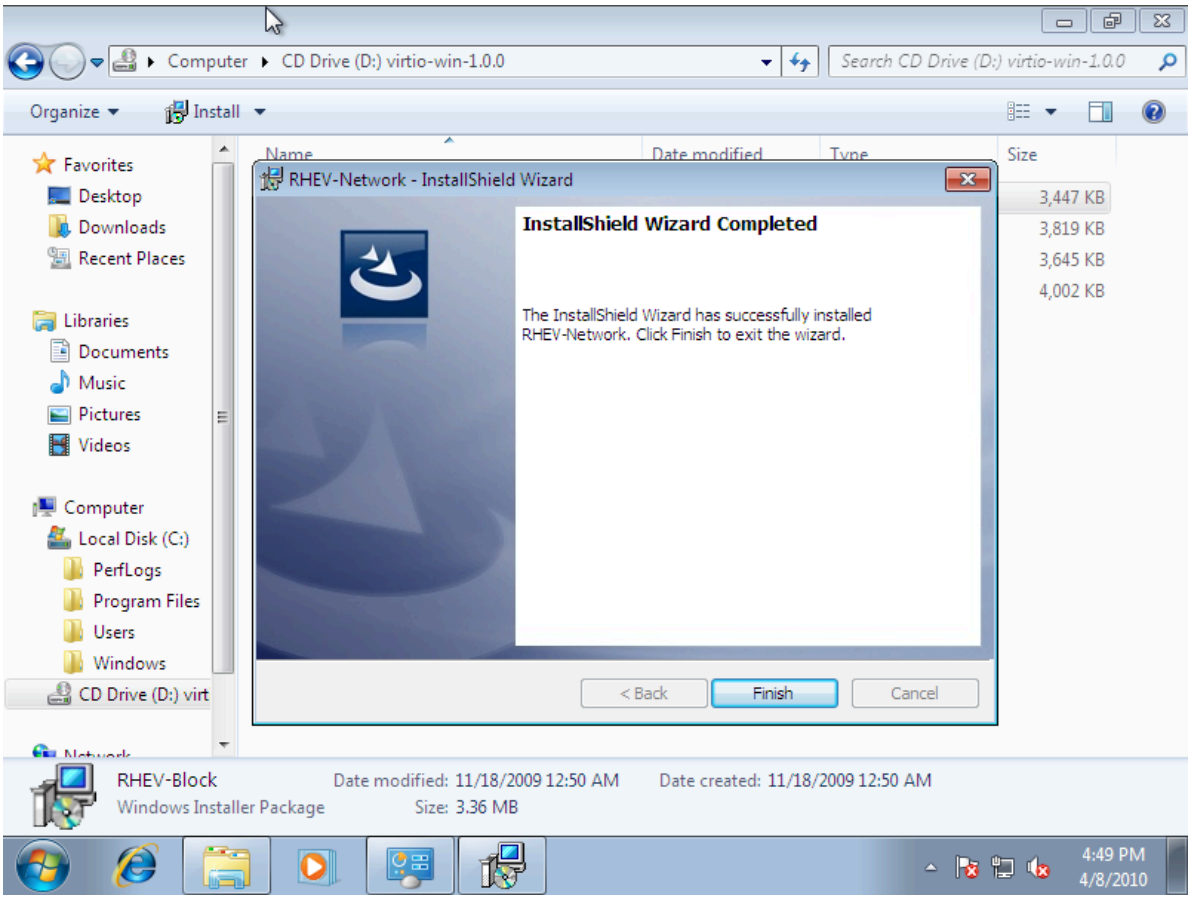
Presione el botón **Next** para continuar.

c. **Confirme la excepción**
Windows podría preguntarle por una excepción de seguridad.


User Account Control
Do you want to allow the following program to install software on this computer?
Program name: 1a265.msi
Verified publisher: Red Hat Inc.
File origin: CD/DVD drive
Show details
Yes
No
Change when these notifications appear

Presione **Yes** si es correcto.

d. **Finalizar**



Presione **Finalizar** para completar la instalación.

5. **Reinicie**
   Reinicie el huésped para completar la instalación de los controladores.

Modifique la configuración del dispositivo para poder utilizar los controladores para-virtualizados (*Sección 12.3, "Uso de controladores KVM para-virtualizados para dispositivos existentes"*), o instale un nuevo dispositivo que utilice los controladores para-virtualizados (*Sección 12.4, "Uso de controladores KVM para-virtualizados para nuevos dispositivos"*).

12.2. Cómo instalar controladores con un disquete virtualizado

Este procedimiento cubre la instalación de controladores para-virtualizados durante una instalación de Windows.

- Tras instalar el VM de Windows por primera vez mediante el menú de ejecución de una sola vez añada **`viostor.vfd`** como un disquete

  a. **Windows Server 2003**
     Cuando Windows le pida pulsar F6 para controladores de tercera parte, hágalo y siga las instrucciones en pantalla.

  b. **Windows Server 2008**
     Cuando el instalador le solicite el controlador, haga clic en **Cargar controlador**, dirija al instalador hacia el dispositivo A:, y seleccione el controlador que se ajuste a su sistema operativo y a su arquitectura.

12.3. Uso de controladores KVM para-virtualizados para dispositivos existentes

Modifique un dispositivo existente de disco duro asociado al huésped para poder utilizar el controlador **`virtio`** en lugar del controlador virtualizado IDE. En el ejemplo que mostramos a continuación se modifican los archivos de configuración libvirt. De manera alternativa, **`virt-manager`**, **`virsh attach-disk`** o **`virsh attach-interface`** pueden añadir un nuevo dispositivo mediante los controladores para-virtualizados *Sección 12.4, "Uso de controladores KVM para-virtualizados para nuevos dispositivos"*.

1. A continuación está el dispositivo de bloque basado en archivo utilizando el controlador IDE virtualizado. Esta es una entrada típica para un huésped virtualizado que no utiliza controladores para-virtualizados.

```
<disk type='file' device='disk'>
   <source file='/var/lib/libvirt/images/disk1.img'/>
   <target dev='hda' bus='ide'/>
</disk>
```

2. Cambie la entrada para usar el dispositivo para-virtualizado modificando la entrada **bus=** para **`virtio`**.

```
<disk type='file' device='disk'>
   <source file='/var/lib/libvirt/images/disk1.img'/>
   <target dev='hda' bus='virtio'/>
</disk>
```

12.4. Uso de controladores KVM para-virtualizados para nuevos dispositivos

Este procedimiento cubre la creación de nuevos dispositivos mediante los controladores para-virtualizados con **`virt-manager`**.

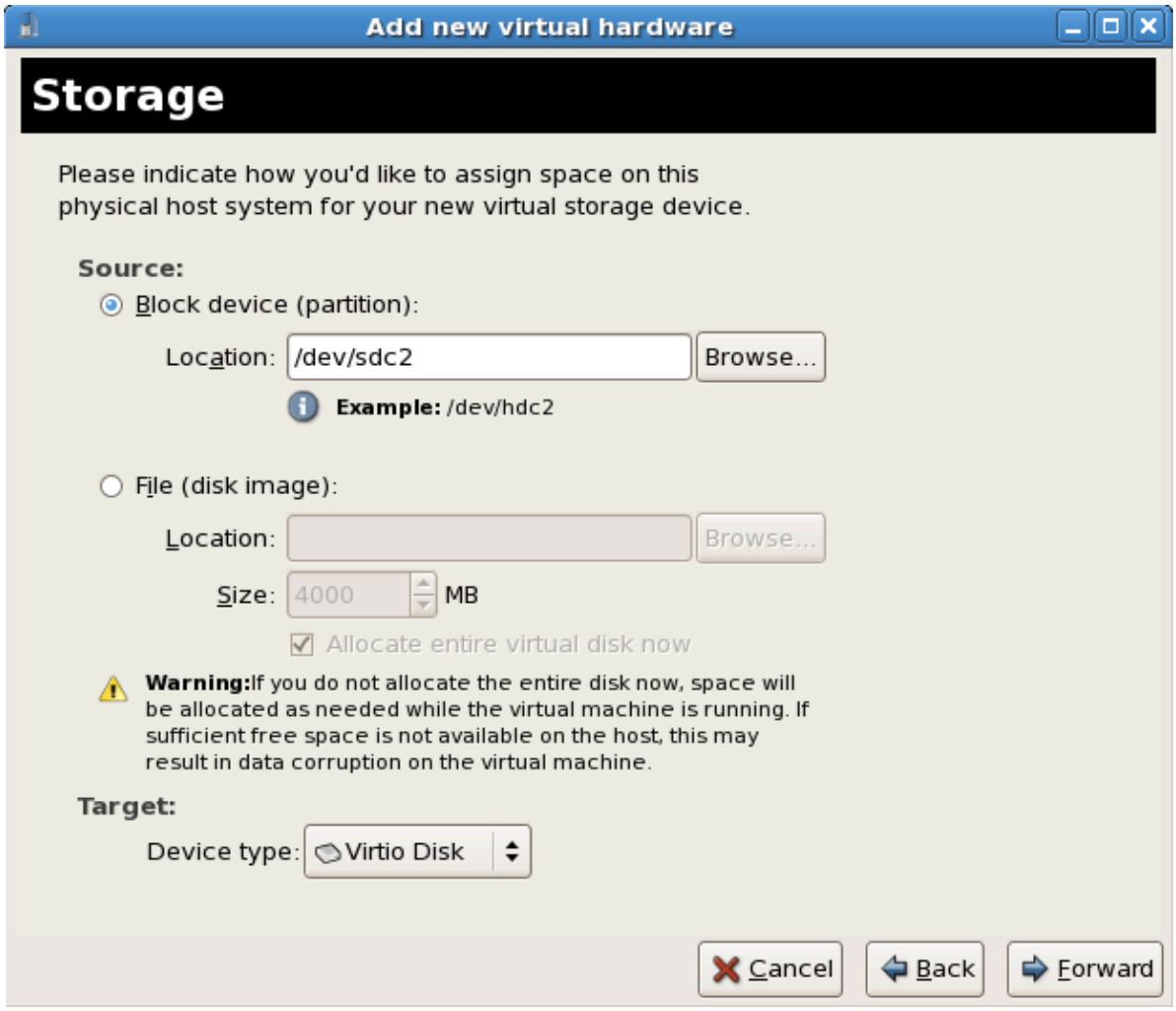
Como alternativa, los comandos**`virsh attach-disk`** o **`virsh attach-interface`** se pueden utilizar para añadir dispositivos mediante los controladores para-virtualizados.

Instale los controladores virtuales primero

Asegúrese que los controladores hayan sido instalados en el huésped de Windows antes de proseguir a instalar nuevos dispositivos. Si los controladores no están disponibles, el dispositivo no será identificado y no funcionará.

1. Abrir el huésped virtualizado al hacer doble clic en el nombre del huéspede en **`virt-manager`**.
2. Abrir la pestaña **Hardware**.
3. Pulse el botón **Agregar Hardware**.
4. En la pestaña de Agregar hardware virtual seleccione **Almacenamiento** o **Red** para el tipo de dispositivo.
    1. **Nuevos dispositivos de disco**

        Seleccione el dispositivo de almacenamiento o archivo de imagen. Seleccione **Disco Virtio** como el **Tipo de dispositivo** y pulse **Adelante**.

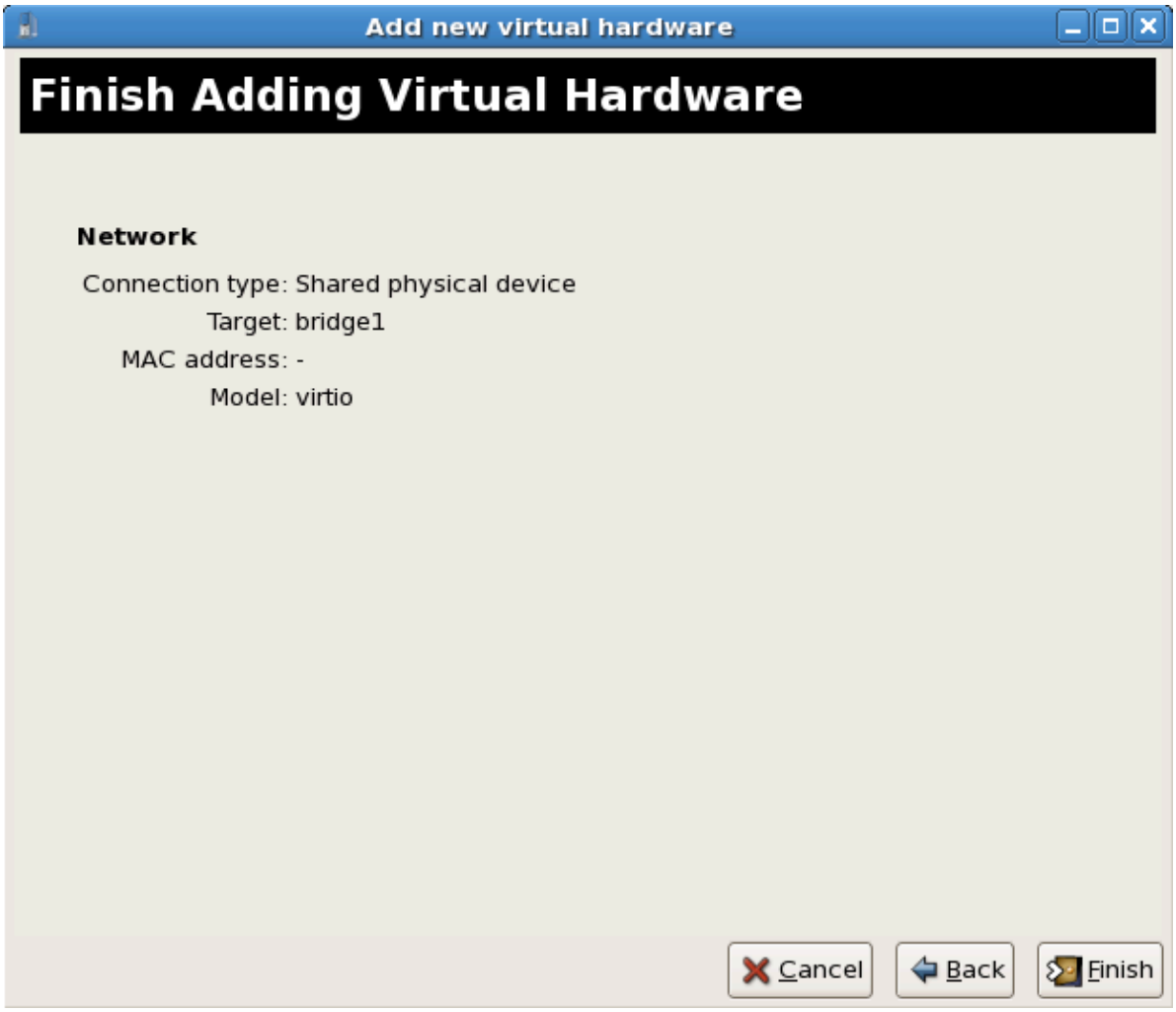

Add new virtual hardware
Storage
Please indicate how you'd like to assign space on this physical host system for your new virtual storage device.
Source:
Block device (partition):
Location: /dev/sdc2
Browse...
Example: /dev/hdc2
File (disk image):
Location:
Browse...
Size: 4000 MB
Allocate entire virtual disk now
Warning: If you do not allocate the entire disk now, space will be allocated as needed while the virtual machine is running. If sufficient free space is not available on the host, this may result in data corruption on the virtual machine.
Target:
Device type: Virtio Disk
Cancel
Back
Forward

2. **Nuevos dispositivos de red**

   Seleccione **Red virtual** o **Dispositivo físico compartido**. Seleccione **virtio** como el **Tipo de dispositivo** y presione **Adelante**.

Add new virtual hardware
Network
Please indicate how you'd like to connect your new virtual network device to the host network.
Virtual network
Network: default
Tip: Choose this option if your host is disconnected, connected via wireless, or dynamically configured with NetworkManager.
Shared physical device
Device: eth1 (Bridge bridge1)
Tip: Choose this option if your host is statically connected to wired ethernet, to gain the ability to migrate the virtual machine.
Set fixed MAC address for this NIC?
MAC address:
Device Model: virtio
Cancel
Back
Forward

5. Presione **Terminar** para guardar el dispositivo.



6. Reinicie el huésped. El dispositivo podría no ser reconocido hasta que el huésped Windows sea reiniciado.

Puente PCI

Este capítulo describe la utilización de los puentes PCI con KVM.

El hipervisor KVM ofrece soporte para asociar al huésped virtualizado, dispositivos PCI del equipo anfitrión. Esto se denomina puente PCI y permite que los huéspedes tengan acceso exclusivo a los dispositivos PCI para una multiplicidad de tareas. Los puentes PCI permiten a los dispositivos PCI ser visualizados y comportarse como si estuvieran físicamente asociados con el sistema operativo del huésped.

Los dispositivos PCI se encuentran limitados por la arquitectura del sistema virtualizado. De los 32 dispositivos PCI disponibles de un huésped, 2 no son removibles. Esto significa que existen disponibles hasta 30 slots PCI por huésped. Cada dispositivo PCI puede cumplir hasta 8 funciones; y algunos tienen múltiples funciones y utilizan sólo un slot. Redes para-virtualizadas, dispositivos de discos para-virtualizados, o cualquier otro dispositivo PCI que utilice la extensión VT-d, utilizan slots o funciones. La cantidad exacta de funciones disponible es difícil de calcular debido a la cantidad de dispositivos posibles. Cada huésped puede utilizar hasta 32 dispositivos PCI, y cada uno de ellos puede desempeñar hasta 8 funciones.

Las extensiones VT-d o AMD IOMMU deben ser habilitadas en el BIOS.

Procedimiento 13.1. Cómo preparar un sistema Intel para utilizar puentes PCI

1. **Habilite las extensiones Intel VT-d**

   Las extensiones Intel VT-d ofrecen soporte de hardware para asignar directamente un dispositivo físico a un huésped. El principal beneficio de este recurso es el de mejorar el desempeño nativo para el acceso de los dispositivos.

   Las extensiones VT-d son necesarias para poder utilizar puentes PCI en Fedora. Las extensiones deben estar habilitadas en el BIOS. Algunos fabricantes de sistemas deshabilitan estas extensiones en forma predeterminada.

   These extensions are often called various terms in BIOS which differ from manufacturer to manufacturer. Consult your system manufacturer's documentation.

2. **Activar Intel VT-d en el kernel**

   Active Intel VT-d en el kernel agregando el parámetro *intel_iommu=on* a la línea del kernel del archivo **/boot/grub/grub.conf**.

   El ejemplo que mostramos a continuación es un archivo **grub.conf** modificado con Intel VT-d activado.

```
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Fedora Server (2.6.18-190.el5)
        root (hd0,0)
        kernel /vmlinuz-2.6.18-190.el5 ro root=/dev/VolGroup00/LogVol00 rhgb
 quiet intel_iommu=on
        initrd /initrd-2.6.18-190.el5.img
```

3. **Listo para ser utilizado**
   Reinicie el sistema para habilitar las modificaciones. Su sistema ahora es capaz de utilizar puentes PCI.

Procedimiento 13.2. Cómo preparar un sistema AMD para utilizar puentes PCI

- **Habilite las extensiones AMD IOMMU**
  Las extensiones AMD IOMMU son necesarias para poder utilizar puentes PCI en Fedora. Estas extensiones deben estar habilitadas en el BIOS, y algunos fabricantes de sistemas las deshabilitan extensiones en forma predeterminada.

Los sistemas AMD sólo necesitan que IOMMU se encuentre habilitado en el BIOS. Una vez que IOMMU se encuentre habilitado, el sistema estará listo para utilizar puentes PCI.

13.1. Cómo agregar un dispositivo PCI com virsh

Los siguientes pasos describen cómo agregar un dispositivo PCI a un huésped completamente virtualizado, en un hipervisor KVM utilizando puentes PCI asistidos por hardware.

Importante
Las extensiones VT-d o AMD IOMMU deben ser habilitadas en el BIOS.

El siguiente ejemplo utiliza un dispositivo de controlador USB con el código de identificación PCI **`pci_8086_3a6c`**, y un huésped completamente virtualizado deominado *`win2k3`*.

1. **Identique el dispositivo**
   Identifique el dispositivo PCI designado para el puente con el huésped. El comando **`virsh nodedev-list`** muestra todos los dispositivos asociados en el sistema. La opción **`--tree`** es útil para identificar otros dispositivos asociados a un dispositivo PCI (por ejemplo, coltroladores de disco y controladores USB).

   ```
   # virsh nodedev-list --tree
   ```

   Para obtener una lista exclusivamente con dispositivos PCI, ejecute el siguiente comando:

   ```
   # virsh nodedev-list | grep pci
   ```

   Cada dispositivo PCI es identificado con una cadena con el siguiente formato (donde *`****`* es un número de cuatro dígitos de código hexadecimal):

   ```
   pci_8086_****
   ```

   Consejo: cómo determinar el dispositivo PCI
   Comparar la salida **`lspci`** con la salida **`lspci -n`** (que deshabilita la resolución de nombres) puede ayudar a deducirr qué dispositivo posee qué código de identificación.

Grabe el número de dispositivo PCI; dicho número será necesario en otras etapas.

2. Información sobre el dominio, bus y funciones, se encuentran disponibles en el resultado del comando **`virsh nodedev-dumpxml`**:

```
# virsh nodedev-dumpxml pci_8086_3a6c
<device>
  <name>pci_8086_3a6c</name>
  <parent>computer</parent>
  <capability type='pci'>
    <domain>0</domain>
    <bus>0</bus>
    <slot>26</slot>
    <function>7</function>
    <id='0x3a6c'>82801JD/DO (ICH10 Family) USB2 EHCI Controller #2</product>
    <vendor id='0x8086'>Intel Corporation</vendor>
  </capability>
</device>
```

3. Desconecte el dispositivo del sistema. Los dispositivos asociados no pueden ser utilizados, y si no son desconectados primero, podrían provocar numerosos errores al huésped.

```
# virsh nodedev-dettach pci_8086_3a6c
Device pci_8086_3a6c dettached
```

4. Convert slot and function values to hexadecimal values (from decimal) to get the PCI bus addresses. Append "0x" to the beginning of the output to tell the computer that the value is a hexadecimal number.

   Por ejemplo, si el bus es = 0, slot = 26, y función = 7, ejecute lo siguiente:

```
$ printf %x 0
0
$ printf %x 26
1a
$ printf %x 7
7
```

   Los valores a ser utilizaods:

```
bus='0x00'
slot='0x1a'
function='0x7'
```

5. Run **`virsh edit`** (or virsh attach device) and added a device entry in the **`<devices>`** section to attach the PCI device to the guest. Only run this command on offline guests. Fedora does not support hotplugging PCI devices at this time.

```
# virsh edit win2k3
<hostdev mode='subsystem' type='pci' managed='yes'>
  <source>
      <address domain='0x0000' bus='0x00' slot='0x1a' function='0x7'/>
  </source>
</hostdev>
```

6. Una vez que el sistema se encuentre configurado para utilizar direcciones PCI, necesitamos indicarle al sistema del equipo anfitrión que deje de utilizarlo. El controlador **ehci** es cargado de manera predeterminada para el controlador PCI USB.

```
$ readlink /sys/bus/pci/devices/0000\:00\:1d.7/driver
../../../bus/pci/drivers/ehci_hcd
```

7. Desasocie el dispositivo:

```
$ virsh nodedev-dettach pci_8086_3a6c
```

8. Verifique que ahora se encuentre bajo el control de pci_stub:

```
$ readlink /sys/bus/pci/devices/0000\:00\:1d.7/driver
../../../bus/pci/drivers/pci-stub
```

9. Defina un valor booleano de SELinux para permitir la administración del dispositivo desde el huésped:

```
$ setsebool -P virt_manage_sysfs 1
```

10. Inicie el sistema huésped:

```
# virsh start win2k3
```

Ahora el dispositivo PCI debería haberse asociado exitosamente al huésped, y poder ser accedido desde el sistema operativo huésped.

13.2. Cómo agregar un dispositivo PCI con virt-manager

Los dispositivos PCI pueden ser agregados a los huéspedes utilizando la herramienta gráfica **virt-manager**. El procedimiento siguiente agrega dos controladores de puertos USB en un huésped virtualizado.

1. **Identique el dispositivo**
   Identifique el dispositivo PCI designado para el puente con el huésped. El comando **virsh nodedev-list** muestra todos los dispositivos asociados en el sistema. La opción **--tree** es útil para identificar otros dispositivos asociados a un dispositivo PCI (por ejemplo, coltroladores de disco y controladores USB).

   ```
   # virsh nodedev-list --tree
   ```

   Para obtener una lista exclusivamente con dispositivos PCI, ejecute el siguiente comando:

   ```
   # virsh nodedev-list | grep pci
   ```

   Cada dispositivo PCI es identificado con una cadena con el siguiente formato (donde ****** es un número de cuatro dígitos de código hexadecimal):

   ```
   pci_8086_****
   ```

Consejo: cómo determinar el dispositivo PCI

Comparar la salida **`lspci`** con la salida **`lspci -n`** (que deshabilita la resolución de nombres) puede ayudar a deducirr qué dispositivo posee qué código de identificación.

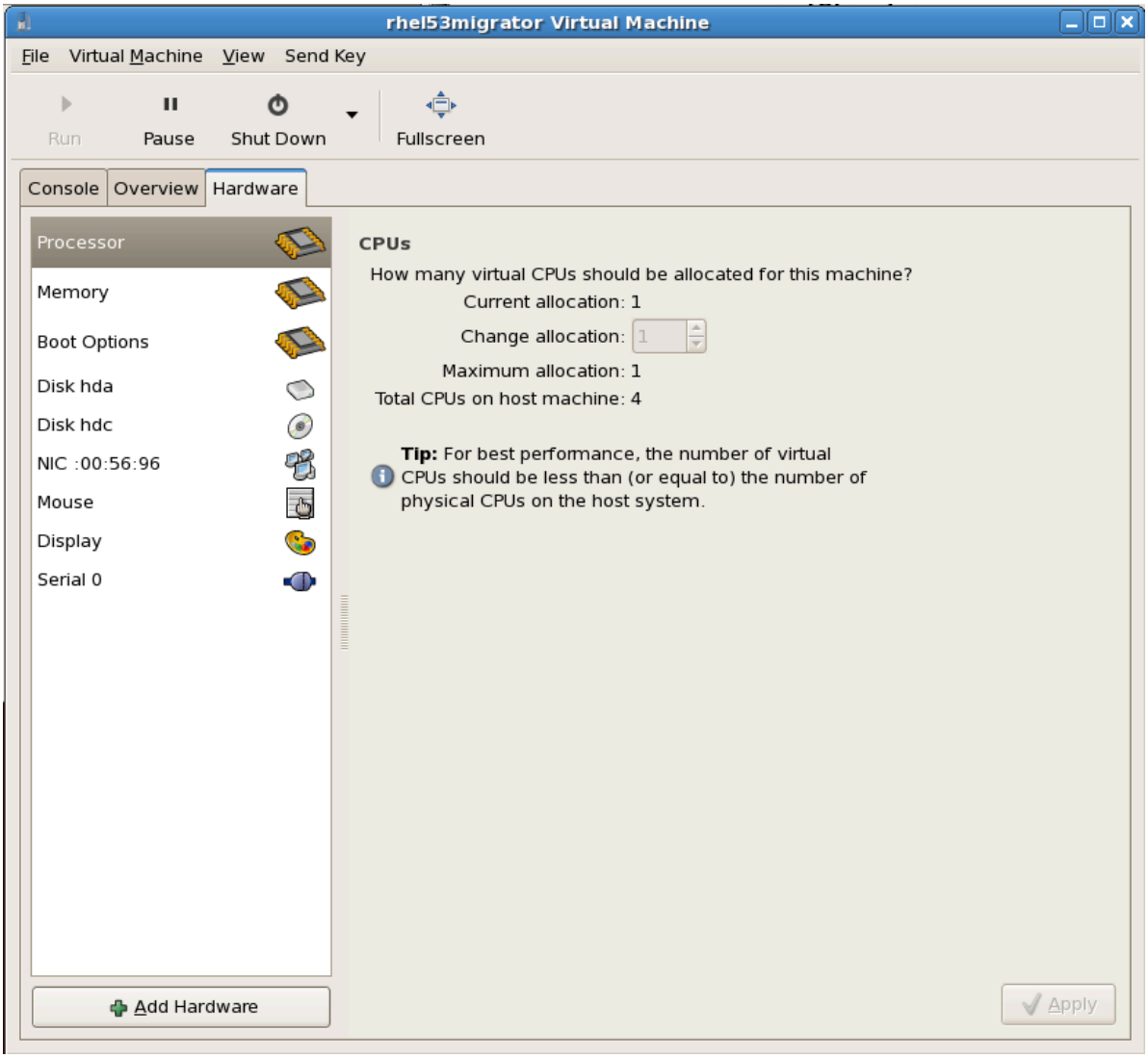
Grabe el número de dispositivo PCI; dicho número será necesario en otras etapas.

2. **Desasocie el dispositivo PCI**
   Desasocie el dispositivo PCI del sistema.

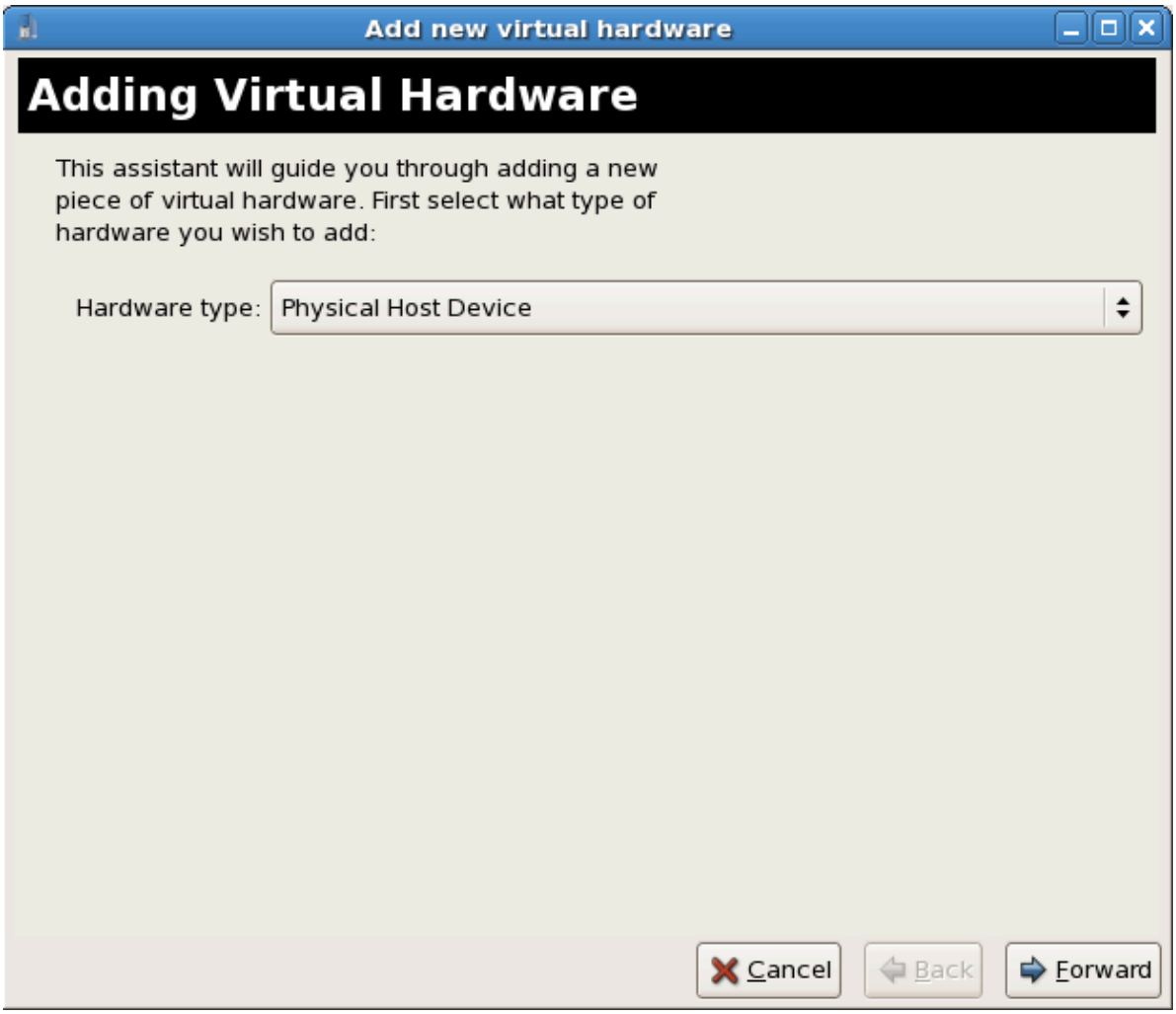
```
# virsh nodedev-dettach pci_8086_3a6c
Device pci_8086_3a6c dettached
```

3. **Desconecte el huésped**
   Desconecte el huésped. La conexión directa de dispositivos PCI en huéspedes que se encuentran funcionado es aún experimental y podría provocar una caída del sistema.

4. **Abra las configuraciones de hardware**
   Abra la máquina virtual y seleccione la pestaña de **Hardware**. Haga clic sobre el botón **Agregar hardware**, para agregar un nuevo dispositivo al huésped.



5. **Agregue el nuevo dispositivo**
   Seleccione **Dispositivo de equipo físico** desde la lista de **Tipo de hardware**. El elemento **Dispositivo de equipo físico** representa los dispositivos PCI. Haga clic en **Adelante**.


Add new virtual hardware
Adding Virtual Hardware
This assistant will guide you through adding a new piece of virtual hardware. First select what type of hardware you wish to add:
Hardware type:
Physical Host Device
Cancel
Back
Forward

6. **Seleccione un dispositivo PCI**
   Elija un dispositivo PCI que se encuentre sin utilizar. Tenga en cuenta que seleccionar dispositivos PCI presentes en el equipo anfitrión y que estén siendo utilizados por éste, causará errores. En nuestro ejemplo es utilizado un dispositivo de interfaz PCI a USB.

7. **Confirme el nuevo dispositivo**
   Haga clic sobre el botón **Finalizar** para confirmar la configuración del dispositivo, y agréguelo al huésped.

La configuración ha sido completada, y ahora el huésped puede utilizar el dispositivo PCI.

13.3. Puentes PCI con virt-install

Para poder utilizar puentes PCI con el parámetro virt-install, utilice el parámetro adicional *--host-device*.

1. **Identifique el dispositivo PCI**
   Identifique el dispositivo PCI designado para el puente con el huésped. El comando **virsh nodedev-list** muestra todos los dispositivos asociados en el sistema. La opción **--tree** es útil para identificar otros dispositivos asociados a un dispositivo PCI (por ejemplo, coltroladores de disco y controladores USB).

   ```
   # virsh nodedev-list --tree
   ```

   Para obtener una lista exclusivamente con dispositivos PCI, ejecute el siguiente comando:

   ```
   # virsh nodedev-list | grep pci
   ```

Cada dispositivo PCI es identificado con una cadena con el siguiente formato (donde ****** es un número de cuatro dígitos de código hexadecimal):

```
pci_8086_****
```

Consejo: cómo determinar el dispositivo PCI

Comparar la salida **lspci** con la salida **lspci -n** (que deshabilita la resolución de nombres) puede ayudar a deducirr qué dispositivo posee qué código de identificación.

2. **Agregue el dispositivo**

   Utilice la salida del identificador PCI del comando **virsh nodedev** como el valor a ser utilizado para el parámetro *--host-device*.

```
# virt-install \
 -n hostdev-test -r 1024 --vcpus 2 \
 --os-variant fedora11 -v --accelerate \
 -l http://download.fedoraproject.org/pub/fedora/linux/development/x86_64/os \
 -x 'console=ttyS0 vnc' --nonetworks --nographics  \
 --disk pool=default,size=8 \
 --debug --host-device=pci_8086_10bd
```

3. **Complete la instalación**

   Complete la instalación del huésped. El dispositivo PCI debería haberse asociado al huésped.

SR-IOV

14.1. Introducción

El SIG PCI (Grupo de interés especial PCI) ha desarrollado la especificación de virtualización de E/S de raíz única (SR-IOV por las iniciales en inglés de Single Root I/O Virtualization). Esta especificación es un estándar para un tipo de puentes PCI que comparten en forma nativa un dispositivo entre varios huéspedes. SR-IOV no necesita de la presencia de un hipervisor en la transferencia y administración de los datos ya que contiene interruptores, flojos DMA, y espacio de memoria indenpendiente para ser utilizados con los huéspedes virtualizados.

SR-IOV habilita una Función de raíz única (por ejemplo, un único puerto Ethernet), para poder figurar como múltiples dispositivos físicos diferentes. Un dispositivo físico com capacidades SR-IOV puede ser configurado para aparecer dentro del espacio de configuración PCI como teniendo funciones múltiples, y cada dispositivo posee su propio espacio de configuración completo con Registros de direcciones base (BARs, por las iniciales en inglés de Base Address Registers).

SR_IOV utiliza dos nuevas funciones PCI:

- Las Funciones físicas (PFs, por las iniciales en inglés de Physical Functions) son dispositivos PCIe completos que ofrecen las capacidades SR-IOV. Las Funciones físicas son descubiertas, administradas y configuradas como dispositivos PCI normales. Las Funciones físicas configuran y administran la funcionalidad de SR-IOV asignándole Funciones virtuales.
- Las Funciones virtuales (VFs, por las iniciales en inglés de Virtual Functions) son funciones PCIe simples que sólo procesan E/S. Cada función virtual es derivada a partir de una Función física. La cantidad de Funciones virtuales que puede tener un dispositivo está limitada por el dispositivo de hardware. Un puerto Ethernet, el Dispositivo físico, puede mapear a varias Funciones virtuales que pueden ser compartidas con los huéspedes virtualizados.

The hypervisor can map one or more Virtual Functions to a virtualized guest. The Virtual Function's configuration space is mapped to the configuration space presented to the virtualized guest by the hypervisor.

Cada Función virtual puede ser mapeada solamente una vez, ya que las Funciones virtuales necesitan de hardware real. Un huésped virtualizado puede tener Funciones virtuales múltiples. Una función virtual aparece como una tarjeta de red en la misma manera en cómo aparecería en un sistema operativo una tarjeta de red común y corriente.

Los controladores SR-IOV son implementados en el kernel. El núcleo de esta implementación está contenido en el subsistema PCI, pero también debe existir un soporte para el controlador tanto de los dispositivos de la función física (PF) como de los de la Función virtual (VF). Con un dispositivo SR-IOV adecuado, es posible alojar VFs a partir de una PF. Las VFs aparecen como dispositivos PCI los que están respaldados por recursos (conjuntos de registros y de colas).

Ventajas de SR-IOV

Los dispositivos SR-IOV pueden compartir un mismo puerto físico con diferentes huéspedes virtualizados.

Las Funciones virtuales ofrecen un desempeño casi nativo, mejor que el ofrecido por controladores para-virtualizados o de acceso emulado. Las funciones virtuales ofrecen protección de datos entre los

huéspedes virtualizados del mismo servidor físico, ya que los datos están administrados y controlados por el hardware.

Estas funciones ofrecen una mayor densidad a los huéspedes virtualizados en equipos dentro de un centro de datos.

Desventajeas de SR-IOV

Live migration is presently experimental. As with PCI passthrough, identical device configurations are required for live (and offline) migrations. Without identical device configurations, guest's cannot access the passed-through devices after migrating.

14.2. Cómo útilizar SR-IOV

Esta sección describe el proceso de asociar una Función virtual como dispositivo de red adicional a un huésped.

SR-IOV necesita soporte Intel VT-d.

Procedimiento 14.1. Asocie un dispositivo de red SR-IOV

1. **Habilite la extensión Intel VT-d tanto en el BIOS como en el kernel**
   Ignore este paso si la extensión Intel-VT-d ya está habilitada y se encuentre funcionando adecuadamente.

   Si aún no lo está, habilite Intel VT-d en el BIOS. Diríjase a *Procedimiento 13.1, “Cómo preparar un sistema Intel para utilizar puentes PCI”* para obtener asistencia en este proceso.

2. **Verifique que exista soporte**
   Compruebe que haya sido detectado si el dispositivo PCI con capacidades SR-IOV. Nuestro ejemplo muestra una tarjeta de interfaz de red Intel 82576 con soporte para SR-IOV. Utilice el comando **`lspci`** para verificar si el dispositivo fue detectado.

   ```
   # lspci
   03:00.0 Ethernet controller: Intel Corporation 82576 Gigabit Network Connection (rev 01)
   03:00.1 Ethernet controller: Intel Corporation 82576 Gigabit Network Connection (rev 01)
   ```

   Tenga en cuenta que el resultado fue modificado para no mostrar el resto de los dispositivos.

3. **Inicie los módulos SR-IOV del kernel**
   Si el dispositivo funcionara, el módulo del controlador del kernel debería ser cargado automáticamente por el propio kernel. Pueden indicarse parámetros opcionales al módulo utilizando el comando **`modprobe`**. La tarjeta de interfaz de red Intel 82576 utiliza el controlador del módulo del kernel **`igb`**.

   ```
   # modprobe igb [<option>=<VAL1>,<VAL2>,]
   # lsmod |grep igb
   igb    87592  0
   dca    6708    1 igb
   ```

4. **Active las Funciones virtaules**
   El parámetro *`max_vfs`* del módulo **`igb`** aloja la máxima cantidad de Funciones virtuales. El parámetro *`max_vfs`* hace que el controlador se expanda hasta el valor "in" de las Funciones virtuales. Para esta tarjeta en particular, el rango válido recorre los valores de *`0`* a *`7`*.

Elimine el módulo para modificar la variable.

```
# modprobe -r igb
```

Reinicie el módulo con el parámetro *max_vfs* definido en *1*, o en cualquier número de Funciones virtuales hasta el máximo permitido por su dispositivo.

```
# modprobe igb max_vfs=1
```

5. **Inspeccione las nuevas Funciones virtuales**
   Utilizando el comando **lspci**, conozca las flamantes Funciones virtuales asociadas al dispositivo de red Intel 82576.

```
# lspci | grep 82576
03:00.0 Ethernet controller: Intel Corporation 82576 Gigabit Network Connection (rev 01)
03:00.1 Ethernet controller: Intel Corporation 82576 Gigabit Network Connection (rev 01)
03:10.0 Ethernet controller: Intel Corporation 82576 Virtual Function (rev 01)
03:10.1 Ethernet controller: Intel Corporation 82576 Virtual Function (rev 01)
```

   El identificador del dispositivo PCI se encuentra con el parámetro *-n* del comando **lspci**.

```
# lspci -n | grep 03:00.0
03:00.0 0200: 8086:10c9 (rev 01)
# lspci -n | grep 03:10.0
03:10.0 0200: 8086:10ca (rev 01)
```

   La Función física corresponde a **8086:10c9** y la Función virtual a **8086:10ca**.

6. **Encuentre los dispositivos con virsh**
   El servicio libvirt debe encontrar el dispositivo para poder añadirlo al huésped. Utilice el comando **virsh nodedev-list** para conocer los dispositivos de equipo disponibles.

```
# virsh nodedev-list | grep 8086
pci_8086_10c9
pci_8086_10c9_0
pci_8086_10ca
pci_8086_10ca_0
[output truncated]
```

   El número de serie tanto de las Funciones físicas como de las virtuales debería estar en la lista.

7. **Obtenga detalles avanzados**
   El **pci_8086_10c9** es una de las Funciones físicas, y el **pci_8086_10ca_0** es la primera Función virtual correspondiente a esa Dunción física. Utilice el comando **virsh nodedev-dumpxml** para obtener un resultado avanzado para ambos dispositivos.

```
# virsh nodedev-dumpxml pci_8086_10ca
# virsh nodedev-dumpxml pci_8086_10ca_0
<device>
  <name>pci_8086_10ca_0</name>
  <parent>pci_8086_3408</parent>
  <driver>
    <name>igbvf</name>
  </driver>
```

```
  <capability type='pci'>
    <domain>0</domain>
    <bus>3</bus>
    <slot>16</slot>
    <function>1</function>
    <product id='0x10ca'>82576 Virtual Function</product>
    <vendor id='0x8086'>Intel Corporation</vendor>
  </capability>
</device>
```

Nuestro ejemplo añade la Función virtual `pci_8086_10ca_0` al huésped en *Paso 9*. Tenga en cuenta que los parámetros **`bus`**, **`slot`** y **`function`** de la Función virtual, son necesarios para agregar el dispositivo.

8. **Desasocie las Funciones virtuales**
   Los dispositivos asociados a un equipo no pueden ser asociados a los huéspedes. Linux asocia automáticamente nuevos dispositivos en el equipo. Desconecte la Función virtual del equipo de modo que ella pueda ser utilizada por el huésped.

```
# virsh nodedev-dettach pci_8086_10ca
Device pci_8086_10ca dettached
# virsh nodedev-dettach pci_8086_10ca_0
Device pci_8086_10ca_0 dettached
```

9. **Agregue la Función virtual al huésped**
   a. Apague el huésped.

   b. Use the output from the **`virsh nodedev-dumpxml pci_8086_10ca_0`** command to calculate the values for the configuration file. Convert slot and function values to hexadecimal values (from decimal) to get the PCI bus addresses. Append "0x" to the beginning of the output to tell the computer that the value is a hexadecimal number.

      El dispositivo de ejemplo posee los siguientes valores: bus = 3, slot = 16, y función = 1. Utilice la herramienta **`printf`** para convertir valores decimales a hexadecimales.

```
$ printf %x 3
3
$ printf %x 16
10
$ printf %x 1
1
```

      Este ejemplo utilizaría los siguientes valores en el archivo de configuración:

```
bus='0x03'
slot='0x10'
function='0x01'
```

   c. Abra el archivo de configuración XML con el comando **`virsh edit`**. El ejemplo siguiente edita un huésped denominado *`MyGuest`*.

```
# virsh edit MyGuest
```

d. El editor de textos predeterminado abrirá el archivo de configuración de libvirt para el huésped. Agregue el nuevo dispositivo en la sección **`devices`** del archivo de configuración XML.

```
<hostdev mode='subsystem' type='pci'>
      <source>
        <address bus='0x03' slot='0x10' function='0x01'/>
      </source>
</hostdev>
```

e. Guarde la configuración.

10. **Reinicie**
    Reinicie el huésped para completar la instalación.

```
# virsh start MyGuest
```

El huésped debería iniciarse satisfactoriamente, y ser capaz de detectar una nueva tarjeta de interfaz de red. Esta nueva tarjeta es la Función virtual del dispositivo SR-IOV.

14.3. Cómo solucionar problemas relacionados con SR-IOV

La sección siguiente contiene algunos problemas y soluciones que podrían afectar a SR-IOV.

Error al iniciar el huésped

Al iniciar la mv configurada, un error reportado es el siguiente:

```
# virsh start test
error: Failed to start domain test
error: internal error unable to start guest: char device redirected to
/dev/pts/2
get_real_device: /sys/bus/pci/devices/0000:03:10.0/config: Permission denied
init_assigned_device: Error: Couldn't get real device (03:10.0)!
Failed to initialize assigned device host=03:10.0
```

Este error a menudo es provocado por un dispositivo que ya ha sido asignado a otro huésped, o al equipo mismo.

Frase de acceso del dispositivo USB

sostenedor

Virtualización de ID de N_Port (NPIV, por las iniciales en inglpes de N_Port ID Virtualization)

Pronto.

Administración del tiempo del huésped KVM

La virtualización plantea numerosos desafíos para el tiempo de mantenimiento del huésped. Aquellos que utilizan TSC como fuente de reloj pueden sufrir problemas de sincronización, ya que muchas CPU modernas no poseen un reloj TSC. Los huéspedes que no poseean un tiempo de mantenimiento adecuado pueden tener problemas con algunos procesos y aplicaciones de red, ya que el huésped se ejecutará más rápido o más despacio que el tiempo real, y provocará una falta de soncronización.

KVM soluciona este problema ofreciendo a los huéspedes un reloj para-virtualizado. Alternativamente, algunos huéspedes en futuras versiones de sus sistemas operativos, pueden utilizar otras fuentes de reloj x86 para su sincronización.

Los huéspedes pueden tener varios problemas causados por relojes y contadores inexactos:

- Los relojes pueden no coincidir con el tiempo real que invalida sesiones y afecta redes.
- Los huéspedes con relojes más lentos pueden tener problemas con la migración.

Estos problemas existen en otras plataformas de virtualización y siempre se debe probar el tiempo.

NTP

El demonio de Protocolo de tiempo de red (NTP) debe estar ejecutándose en el host y en los huéspedes. Habilite el servicio `ntpd`:

```
# service ntpd start
```

Añada el servicio ntpd a la secuencia de arranque predeterminada:

```
# chkconfig ntpd on
```

Al utilizar el servicio `ntpd` se deben minimizar los efectos del desplazamiento del reloj en todos los casos

Cómo determinar si su CPU tiene el contador de tiempo de marca constante

Su CPU tiene un contador de marca de tiempo constante si el indicador **`constant_tsc`** está presente. Para determinar si su CPU tiene el indicador **`constant_tsc`**, ejecute el siguiente comando:

```
$ cat /proc/cpuinfo | grep constant_tsc
```

Si se entrega alguna salida su CPU tiene el bit **`constant_tsc`**. Si no hay ninguna salida siga las instrucciones dadas a continuación.

Configuración de hosts sin un contador de tiempo de marca constante

Los sistemas sin contadores de tiempo de marca constante requieren una configuración adicional. Las funciones de administración de energía interfieren con el control preciso de la puntualidad y deben desactivarse para que los huéspedes puedan mantener la puntualidad exacta con KVM.

Nota

Estas instrucciones son para la revisión de AMD únicamente CPU de F.

Si la CPU carece del bit **constant_tsc**, deshabilite todas las herramientas de administración de energía (*BZ#513138*[1]). Cada sistema tiene varios contadores que sirven para controlar el tiempo. El TSC no es estable en el equipo, lo cual se debe, algunas veces, a cambios de **cpufreq**, estado deep C, o migración a un equipo con un TSC más rápido. Para evitar que el kernel utilice estados deep C, que pueden detener el TSC, añada "**processor.max_cstate=1**" a las opciones de arranque del kernel en el archivo **grub.conf** del equipo:

```
term Red Hat Enterprise Linux Server (2.6.18-159.el5)
        root (hd0,0)
 kernel /vmlinuz-2.6.18-159.el5 ro root=/dev/VolGroup00/LogVol00 rhgb
 quiet processor.max_cstate=1
```

Desactive **cpufreq** (sólo necesario en sin **constant_tsc**) editando el archivo de configuración **/etc/sysconfig/cpuspeed** y cambiando las variables **MIN_SPEED** y **MAX_SPEED** a la frecuencia más alta disponible. Los límites válidos se pueden encontrar en los archivos **/sys/devices/system/cpu/cpu*/cpufreq/scaling_available_frequencies**.

Uso del reloj para-virtualizado con huéspedes de Red Hat Enterprise Linux

Para algunos huéspedes de Red Hat Enterprise Linux, se requieren parámetros de kernel adicionales. Dichos parámetros se pueden establecer añadiéndolos al final de la línea de /kernel en el archivo /boot/grub/grub.conf del huésped.

La tabla que ofrecemos a continuación presenta versiones de Fedora y parámetros requeridos por los equipos en sistemas que no posean un contador de marca de tiempo constante.

Red Hat Enterprise Linux	Parámetros adicionales del kernel huésped
5.4 AMD64/Intel 64 con el reloj para-virtualizado	No se requieren parámetros adicionales
5.4 AMD64/Intel 64 sin el reloj para-virtualizado	divider=10 notsc lpj=n
5.4 x86 con el reloj para-virtualizado	No se requieren parámetros adicionales
5.4 x86 sin el reloj para-virtualizado	divider=10 clocksource=acpi_pm lpj=n
5.3 AMD64/Intel 64	divider=10 notsc
5.3 x86	divider=10 clocksource=acpi_pm
4.8 AMD64/Intel 64	notsc divider=10
4.8 x86	clock=pmtmr divider=10
3.9 AMD64/Intel 64	No se requieren parámetros adicionales
3.9 x86	No se requieren parámetros adicionales

[1] https://bugzilla.redhat.com/show_bug.cgi?id=513138

Cómo utilizar RTC con huéspedes Windows Server 2003 y Windows XP

Windows utiliza dos relojes: el Reloj de tiempo real (RTC, por las iniciales en inglés de Real-Time Clock), y Contador de marca de tiempo (TSC, Time Stamp Counter). Para los huéspedes Windows RTC puede ser utilizado en lugar del TSC para todas las fuentes de tiempo, ya que el RTC resuelve los problemas de sincronización.

Para habilitar la fuente de reloj PMTIMER en RTC (Generalmente, PMTIMER utiliza TSC), agregue la línea siguiente a las configuraciones de arranque de Windows. Estas configuraciones están almacenadas en el archivo boot.ini. Agregue la siguiente línea al archivo **`boot.ini`**:

```
/use pmtimer
```

Para obtener mayor información sobre arranque en Windows y la opción pmtimer, consulte *Opciones disponibles de cambio para Windows XP y los archivos Windows Server 2003 Boot.ini files*[2].

Cómo utilizar el Reloj de tiempo real (RTC) con huéspedes Windows Vista, Windows Server 2008 y Windows 7.

Windows utiliza dos relojes: el Reloj de tiempo real (RTC, por las iniciales en inglés de Real-Time Clock), y Contador de marca de tiempo (TSC, Time Stamp Counter). Para los huéspedes Windows RTC puede ser utilizado en lugar del TSC para todas las fuentes de tiempo, ya que el RTC resuelve los problemas de sincronización.

El archivo **`boot.ini`** ya no es utilizado a partir de Windows Vista, y de las versiones que le siguen. Windows Vista, Windows Server 2008 y Windows 7, para modificar sus parámetros de arranque, utilizan la herramienta **Editor de datos de configuración de arranque** (**`bcdedit.exe`**).

El procedimiento siguiente solo es necesario si el huésped está presentando problemas de tiempo de mantenimiento. Estos problemas podrían no afectar a los huéspedes de todos los equipos.

1. Abra el huésped Windows.
2. Abra el menú **Accesorios** del menú **Inicio**. Haga clic con el botón secundario sobre la aplicación **Intérprete de comandos**, seleccione **Ejecutar como administrador**.
3. Si se lo solicita, confirme la excpeción de seguridad.
4. Configure el administrador de arranque para que utilice el reloj de plataforma. Esto debería indicarle a Windows que utilice el timer PM con la fuente primaria de reloj. El UUID del sistema (*`{default}`* en el ejemplo a continuación) debería ser modificado si el UUID del sistema es diferente que el dispositivo de arranque predeterminado.

   ```
   C:\Windows\system32>bcdedit /set {default} USEPLATFORMCLOCK on
   The operation completed successfully
   ```

Esta solución debería mejorar el tiempo de mantenimiento para los huéspedes de Windows Vista, Windows Server 2008 y Windows 7.

[2] http://support.microsoft.com/kb/833721

Parte IV. Administración

Administración de sistemas virtualizados

Estos capítulos contienen información para administración del anfitrión y de los invitados virtualizados mediante herramientas incluidas en Fedora.

Mejores prácticas de servidor

Las siguientes tareas y consejos le pueden ayudar a asegurar y garantizar la confiabilidad de su equipo anfitrión Fedora.

- Ejecute SELinux en el modo "Impositivo". Puede activar SELinux con el siguiente comando:

```
# setenforce 1
```

- Remueva o desactive los servicios innecesarios (tales como **AutoFS**, **NFS**, **FTP**, **HTTP**, **NIS**, **telnetd**, **sendmail**, etc.).
- Añada tan sólo las cuentas de usuario necesarias para la administración de la plataforma en el servidor y remueva aquellas que sean innecesarias.
- Evite ejecutar las aplicaciones que no sean esenciales en su host. La ejecución de aplicaciones en el host puede impactar el rendimiento de la máquina virtual y puede afectar la estabilidad del servidor. Cualquier aplicación que pueda dañar el servidor también hará que todas las máquinas virtuales en el servidor se caigan.
- Utilice una ubicación central para las imágenes e instalaciones de las máquinas virtuales. Las imágenes de la máquina virtual deben ser almacenadas bajo**/var/lib/libvirt/images/**. Si utiliza un directorio diferente para las imágenes de la máquina virtual, asegúrese de añadir el directorio a su política de SELinux y de re-etiquetarlo antes de iniciar la instalación.
- Las fuentes de instalación, árboles e imágenes deben ser almacenadas en una ubicación central, usualmente la ubicación de su servidor `vsftpd`.

Seguridad para la virtualización

Al implementar tecnologías de virtualización en la infraestructura de su organización, debe asegurarse de que los equipos no queden comprometidos. El equipo anfitrión es un sistema Fedora que administra el sistema, los dispositivos, la memoria y las redes, y al mismo tiempo, a todos los huéspedes virtualizados. Si el equipo anfitrión es inseguro, el resto de los huéspedes serán vulnerables. Existen varias formas de mejorar la seguridad en sistemas que utilizan virtualización. Usted o su organización deberían crear un *Plan de implementación* que comprenda las especificaciones operativas y especifique qué servicios serán necesarios en sus huéspedes virtualizados y sus servidores de equipo, y al mismo tiempo en todo el soporte necesario para estos servicios. A continuación presentamos algunos problemas de seguridad que habría que considerar durante el desarrollo del plan de implementación:

- Ejecute sólo el número de servicios necesarios en hosts. Entre menos procesos y servicios se estén ejecutando en el host, mayor será el nivel de seguridad y rendimiento requerido.
- Habilite *SELinux* en el hipervisor. Para obtener mayor información en el uso de SELinux y virtualización, lea *Sección 19.2, “SELinux y virtualización completas”*.
- Utilice un cortafuegos para limitar el tráfico a dom0. Puede establecer un cortafuegos con reglas reject predeterminadas que ayuden a asegurar dom0. También es importante limitar los servicios expuestos a la red.
- No permita que usuarios normales tengan acceso a dom0. Si permite que los usuarios normales tengan acceso a dom0, se corre el riesgo de aumentar la vulnerabilidad de dom0. Recuerde, dom0 es privilegiado y su nivel de seguridad se puede ver comprometido por cuentas no privilegiadas si éstas se permiten.

19.1. Problemas en la seguridad del almacenamiento

En determinadas circunstancias, los administradores de huéspedes virtualizados pueden modificar las particiones que el equipo anfitrión inicia. Para evitar esto, los administradores deberían seguir las siguientes recomendaciones:

El equipo anfitrión no debería utilizar etiquetas de disco para identificar el sistema de archivos en los archivos **`fstab`**, **`initrd`**, o cualquier otro utilizado por la línea de comandos del kernel. Llegado el caso que usuarios sin privilegios de admisnitaradores (especialemente los huéspedes virtualizados) tengan acceso de escritura a la totalidad de las particiones, o a volúmenes LVM, el sistema podría estar comprometido.

No debería otorgarse a los huéspedes acceso de escritura a la totalidad de los discos, o a dispositivos de bloque (por ejemplo, **`/dev/sdb`**). Utilice particiones (por ejemplo, **`/dev/sdb1`**), o volúmenes LVM.

19.2. SELinux y virtualización completas

Linux con seguridad mejorada fue desarrollada por laNSA con la ayuda de la comunidad de Linux para proporcionar una mayor seguridad. SELinux limita las herramientas de los atacantes y sirve para evitar muchos ataques a la seguridad tales como ataques de desbordamiento de búfer, o escalada de privilegios. Es debido a estos beneficios que Fedora recomienda que todos los sistemas Linux deberían ejecutarse con SELinux activado en modo impositivo.

SELinux impide la carga de imágenes de huésped, si SELinux está habilitado y las imágenes no están en el directorio correcto. SELinux requiere que todas las imágenes sean almacenadas en **/var/lib/libvirt/images**.

Adición de almacenamiento basado en LVM con SELinux en modo impositivo.

La siguiente sección es un ejemplo de la adición de un volumen lógico a un huésped virtualizado con SELinux habilitado. Estas instrucciones también se aplican a particiones de disco duro.

Procedimiento 19.1. Creación y montaje de un volumen lógico en un huésped virtualizado con SELinux habilitado.

1. Creación de un volumen lógico. Este ejemplo crea un volumen lógico de 5 GB denominado *NewVolumeName* en el grupo de volumen denominado *volumegroup*.

```
# lvcreate -n NewVolumeName -L 5G volumegroup
```

2. De formato al volumen lógico *NewVolumeName* con un sistema de archivos que soporta atributos, tales como ext3.

```
# mke2fs -j /dev/volumegroup/NewVolumeName
```

3. Cree un nuevo directorio para montar el nuevo volumen lógico. Este directorio puede estar en cualquier parte de su sistema de archivos. Se recomienda ponerlo en directorios de sistema importantes (**/etc**, **/var**, **/sys**) o en directorios principales (**/home** o **/root**). Este ejemplo utiliza un directorio llamado **/virtstorage**

```
# mkdir /virtstorage
```

4. Monte el volumen lógico.

```
# mount /dev/volumegroup/NewVolumeName /virtstorage
```

5. Defina el tipo apropiado de SELinux para la carpeta de la imagen de libvirt.

```
# semanage fcontext -a -t virt_image_t "/virtualization(/.*)?"
```

Si se utiliza la política objetivo (la objetivo es la predeterminada por defecto) el comando añadirá una línea al archivo **/etc/selinux/targeted/contexts/files/file_contexts.local**, el cual hace el cambio persistente. La línea añadida puede ser similar a ésta:

```
/virtstorage(/.*)?    system_u:object_r:virt_image_t:s0
```

6. Ejecute el comando para modificar el tipo de punto de montaje (**/virtstorage**) y todos los archivos bajo él para **virt_image_t** (los comando **restorecon** y **setfiles** leen los archivos en **/etc/selinux/targeted/contexts/files/**).

```
# restorecon -R -v /virtualization
```

Probando nuevos atributos

Genere un nuevo archivo en el sistema de archivos (utilizando el comando **touch**).

```
# touch /virtualization/newfile
```

Verifique que el archivo ha sido re etiquetado utilizando el siguiente comando:

```
# sudo ls -Z /virtualization
-rw-------. root root system_u:object_r:virt_image_t:s0 newfile
```

El resultado muestra que el nuevo archivo posee el atributo correcto, **virt_image_t**.

19.3. SELinux

Las siguientes secciones contiene información que debe tenerse en cuenta cuando se utilice SELinux en su implementación de virtualización. Cuando se implementan modificaciones en el sistema, o se agregan dispositivos, debe actualizar su política de SELinux de acuerdo a estas modificaciones. Para configurar un volumen LVM para un huésped, debe modificar el contexto SELinux para el dispositivo de bloque subyacente y el grupo de volumen respectivos.

```
# semanage fcontext -a -t virt_image _t -f -b /dev/sda2
# restorecon /dev/sda2
```

SELinux y KVM

Existen varios booleanos de SELinux que afectan a KVM. A continuación ofrecemos un listado con ellos.

Booleanos de SELinux en KVM

Booleanos de SELinux	Descripción
allow_unconfined_qemu_transition	Predeterminado: desactivado. Este booleano controla si los huéspedes KVM pueden o no transicionar a usuarios no confinados.
qemu_full_network	Predeterminado: on. Este booleano controla el acceso total de red a los huéspedes KVM.
qemu_use_cifs	Default: on. This boolean controls KVM's access to CIFS or Samba file systems.
qemu_use_comm	Predeterminado: on. Este booleano controla si KVM puede o no tener acceso a los puertos de comunicación seriales o paralelos.
qemu_use_nfs	Default: on. This boolean controls KVM's access to NFS file systems.
qemu_use_usb	Predeterminado: on. Este booleano permite a KVM tener acceso a dispositivos USB.

19.4. Información del cortafuegos de virtualización

Varios puertos son utilizados para realizar comunicaciones entre los huéspedes virtualizados y herramientas de administración.

Servicios de red del huésped

Cualquier servicio de red en un huésped virtualizado debe poseer los puertos de aplicación abiertos en el mismo huésped, y de este modo permitir acceso externo. Si un servicio de red en un huésped es detenido por el cortafuegos, será inaccesible. Siempre verifique primero la configuración de red de los huéspedes.

- Las peticiones ICMP deben ser acepatadas. Los paquetes ICMP son utilizados para verificaciones de red. No puede realizar pings a los huéspedes si los paquetes ICMP se encuentran bloqueados.
- El puerto 22 debería estar abierto ára acceso SSH y para la instalación inicial.
- Los puertos 80 o 443 (de acuerdo a las configuraciones de seguridad del administrador RHEV) son utilizados por el servicio vdsm-reg para comunicar información relacionada con el equipo.
- Los puertos existentes entre el 5634 y el 6166 son utilizados para el acceso de la consola del huésped mediante el protocolo SPICE.
- Los puertos existentes entre el 49152 y el 49216 son utilizados para realizar migraciones mediante KVM. La migración puede utilizar cualquier puerto en este rango, dependiendo de la cantidad de migraciones concurrentes que se estén llevando a cabo
- Habilitar el reenvío de IP (`net.ipv4.ip_forward = 1`) es algo también necesario para puentes compartidos y para el puente predeterminado. Tenga en cuenta que al instalar libvirt se habilita esta variable, de modo que estará activa cuando los paquetes de virtualización se encuentren instalados, a menos que se deshabilite manualmente.

Migración en vivo KVM

Este capítulo cubre el tema de huéspedes de migración que se ejecutan en un hipervisor de KVM a otro host de KVM.

Migración es el nombre que se da al proceso de desplazar un huésped virtualizado de un equipo a otro. La migración es una función clave de virtualización puesto que el software está completamente separado del hardware. La migración sirve para:

- Balance de carga - cuando un equipo se encuentre sobrecargado, sus huéspedes pueden ser trasladados a otros equipos con menor utilización.
- Caída de hardware - cuando los dispositivos de hardware de su equipo empiecen a fallar, los huéspedes pueden ser reubicados de manera segura, de modo de poder desconectar y reparar los problemas existentes.
- Ahorro de energía - los huéspedes pueden ser redistribuidos en otros equipos, el sistema anfitrión puede ser desconectado, y poder así ahorrar energía o abaratar costos en períodos de escasa utilización
- Migración geográfica - los equipos pueden ser trasladados hacia otras ubicaciones para disminuir la latencia, o durante circunstancias problemáticas.

Migrations can be performed live or offline. To migrate guests the storage must be shared. Migration works by sending the guests memory to the destination host. The shared storage stores the guest's default file system. The file system image is not sent over the network from the source host to the destination host.

Una migración offline suspende el equipo, y luego traslada la imagen de la memoria del huésped hacia el equipo de destino. Este huésped es reanudado en el equipo de destino y la memoria que utilizaba en el equipo original es liberada.

El tiempo de una migración desconectada depende del ancho de banda y de la latencia. Un huésped con 2GB de memoria debe tomarse un promedio de ten o más segundos en un enlace de Ethernet de 1 Gbit.

Una migración en vivo mantiene al huésped en ejecución en el equipo de origen y comienza a desplazar la memoria sin detenerlo. Todas las páginas modificadas de memoria son controladas en busca de cambios, y enviadas a su destino al mismo tiempo que la imagen es enviada. La memoria es actualizada con las páginas modificadas. El proceso continúa hasta que la cantidad de tiempo de pausa permitido para el huésped sea igual al tiempo esperado para que las últimas páginas sean transferidas. KVM calcula el tiempo restante e intenta transferir la máxima cantidad de archivos de página desde la fuente al destino hasta que se prediga que la cantidad de páginas restantes pueda ser transferida en un período de tiempo muy breve, mientras que el huésped virtualizado está en pcausa. Los registros son cargados en el nuevo equipo y entonces el huésped es reanudado en el equipo de destino. Si el huésped no puede fusionarse (que es lo que sucede cuando la carga es excesiva), se interrumpe y en su lugar se inicia una migración desconectada.

El tiempo que tarda una migración desconectada depende tanto del ancho de banda de la red como de la latencia. Si la red se encuentra siendo utilizada, o si el ancho de banda disponible es escaso, la migración necesitará de mayor cantidad de tiempo.

20.1. Requerimientos de migración en vivo

La migración de huéspedes requiere lo siguiente:

Requerimientos de migración

- Un huésped virtualizado instalado en un almacenaje de red compartido mediante uno de los siguientes protocolos:
  - Canal de fibra
  - iSCSI
  - NFS
  - GFS2
- Dos o más sistemas Fedora, de la misma versión con las mismas actualizaciones.
- Ambos sistemas deben tener los puertos abiertos apropiados.
- Ambos sistemas deben tener configuraciones de red idénticas. Todas las configuraciones de puente y de red deben ser exactamente iguales en ambos hosts.
- El almacenaje compartido debe montarse en la misma ubicación en los sistemas de fuente y destino. El nombre de directorio montado debe ser idéntico.

Configuración de almacenaje de redes

Configure el almacenamiento compartido e instale un huésped en él. Para obtener instrucciones de almacenamiento compartido, consulte *Parte V, “Cuestiones relacionadas con el almacenamiento en virtualización”*.

De manera alternativo, utilice el ejemplo de NFS en *Sección 20.2, “Ejemplo de almacenaje compartido: NFS para una migración sencilla”*.

20.2. Ejemplo de almacenaje compartido: NFS para una migración sencilla

Este ejemplo utiliza NFS para compartir imágenes de huésped con otros hosts de KVM. Este ejemplo no es práctico para instalaciones grandes, este ejemplo es únicamente para demostrar técnicas de migración y pequeñas implementaciones. No utilice este ejemplo para migrar o ejecutar más de unos pocos huéspedes virtualizados.

Para conocer instrucciones más complejas acerca de configuraciones más robustas de almacenamientos, consulte *Parte V, “Cuestiones relacionadas con el almacenamiento en virtualización”*

1. **Exporte su directorio de imagen libvirt**
   Añada el directorio de imagen predeterminado al archivo **`/etc/exports`**:

   ```
   /var/lib/libvirt/images *.example.com(rw,no_root_squash,async)
   ```

   Cambie el parámetro de huéspedes como se requiere para su entorno.

2. **Iniciar NFS**
   a. Instale los paquetes NFS si aún no han sido instalados:

```
# yum install nfs
```

   b. Abra los puertos para NFS en **iptables** y añada NFS al archivo **/etc/hosts.allow**.

   c. Inicie el servicio NFS:

```
# service nfs start
```

3. **Monte el almacenaje compartido de destino**
   En el sistema de destino, monte el directorio **/var/lib/libvirt/images**:

```
# mount sourceURL:/var/lib/libvirt/images /var/lib/libvirt/images
```

Las ubicaciones deben ser las mismas en fuente y destino
Sea cual sea el directorio que se escoja para los huéspedes debe ser exactamente lo mismo en host como en huésped. Esto también se aplica a todos los tipos de almacenaje compartido. El directorio deber ser el mismo o de lo contrario, la migración fallará.

20.3. Migración KVM en vivo con virsh

Un huésped puede ser migrado a otro host con el comando **virsh**. El comando **migrate** acepta parámetros en el siguiente formato:

```
# virsh migrate --live GuestName DestinationURL
```

El parámetro *GuestName* representa el nombre del huésped que desea migrar.

El parámetro *DestinationURL* es la URL o el equipo del sistema de destino. El sistema de destino debe estar utilizando la misma versión de Fedora, el mismo hipervisor, y debe estar ejecutando **libvirt**.

Una vez que el comando sea ingresado, le será solicitada la contraseña de usuario root del sistema de destino

Ejemplo: migración en vivo con virsh

El ejemplo siguiente migra desde `prueba1.ejemplo.com` a `prueba2.ejemplo.com`. Modifique el nombre de los equipos para su entorno. Este ejemplo migra una máquina virtual llamada **RHEL4test**.

El ejemplo siguiente supone que usted tiene completamente configurado el almacenamiento compartido, y que reúne todos los prerequisitos (listados aquí: *Requerimientos de migración*).

1. **Verificar que el huésped esté ejecutándose**
   Desde el sistema origen, `prueba1.ejemplo.com`, verifique si `RHEL4test` se esté ejecutando:

```
[root@test1 ~]# virsh list
```

```
Id Name                 State
----------------------------------
 10 RHEL4                running
```

2. **Migrar el huésped**
   Ejecute el siguiente comando para migrar en vivo el huésped al destino, `prueba2.ejemplo.com`. Añada **`/system`** al final de la URL de destino para decirle a libvirt que usted necesita acceso total.

```
# virsh migrate --live RHEL4test qemu+ssh://test2.example.com/system
```

   Una vez que el comando sea ingresado, le será solicitada la contraseña de usuario root del sistema de destino

3. **Espere**
   La migración puede tomarse algún tiempo dependiendo de la carga y del tamaño del huésped. **`virsh`** sólo reporta errores. El huésped continúa ejecutándose en el host fuente hasta migrar completamente.

4. **Verificar que el huésped haya llegado al host de destino**
   Desde el sistema de destino, `prueba2.ejemplo.com`, verifique que `RHEL4test` esté en ejecución:

```
[root@test2 ~]# virsh list
Id Name                 State
----------------------------------
 10 RHEL4                running
```

La migración en vivo ahora está completa.

Otros métodos de red

Libvirt soporta una gran variedad de métodos de red incluyendo TLS/SSL, unix sockets, SSH, y TCP no cifrado. Consulte *Capítulo 21, Administración remota de huéspedes virtualizados* para obtener mayor información sobre otros métodos.

20.4. Migración con virt-manager

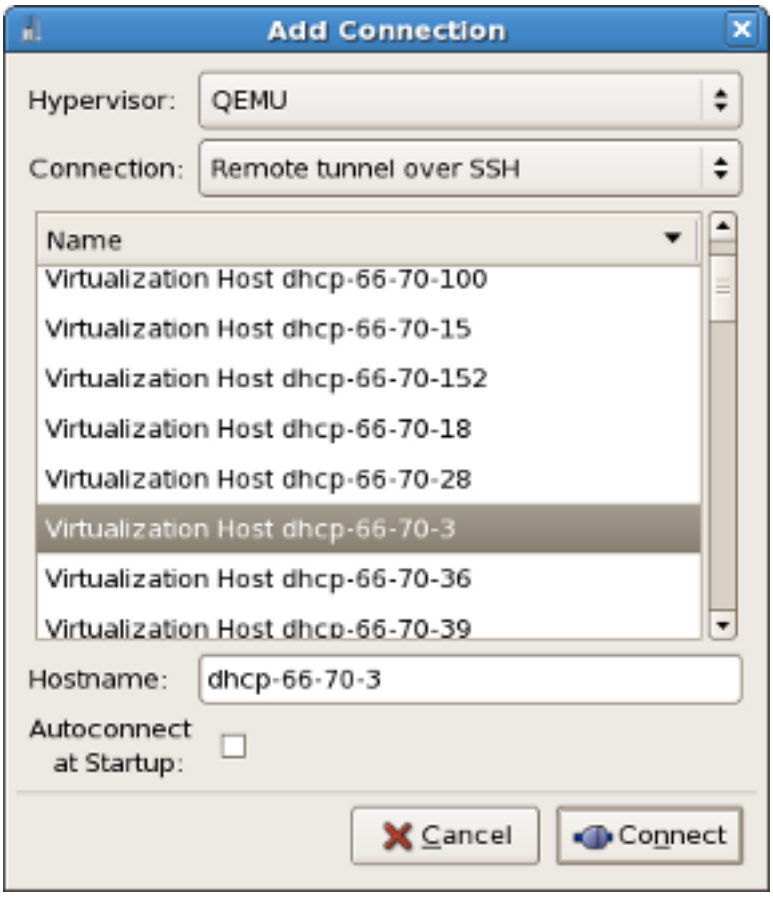
Esta sección cubre la migración de huéspedes basados en KVM con **`virt-manager`**.

1. Conecte a los hosts de origen y destino. En el menú **Archivo**, haga clic en **Añadir conexión**, la ventana **Añadir conexión** aparecerá.

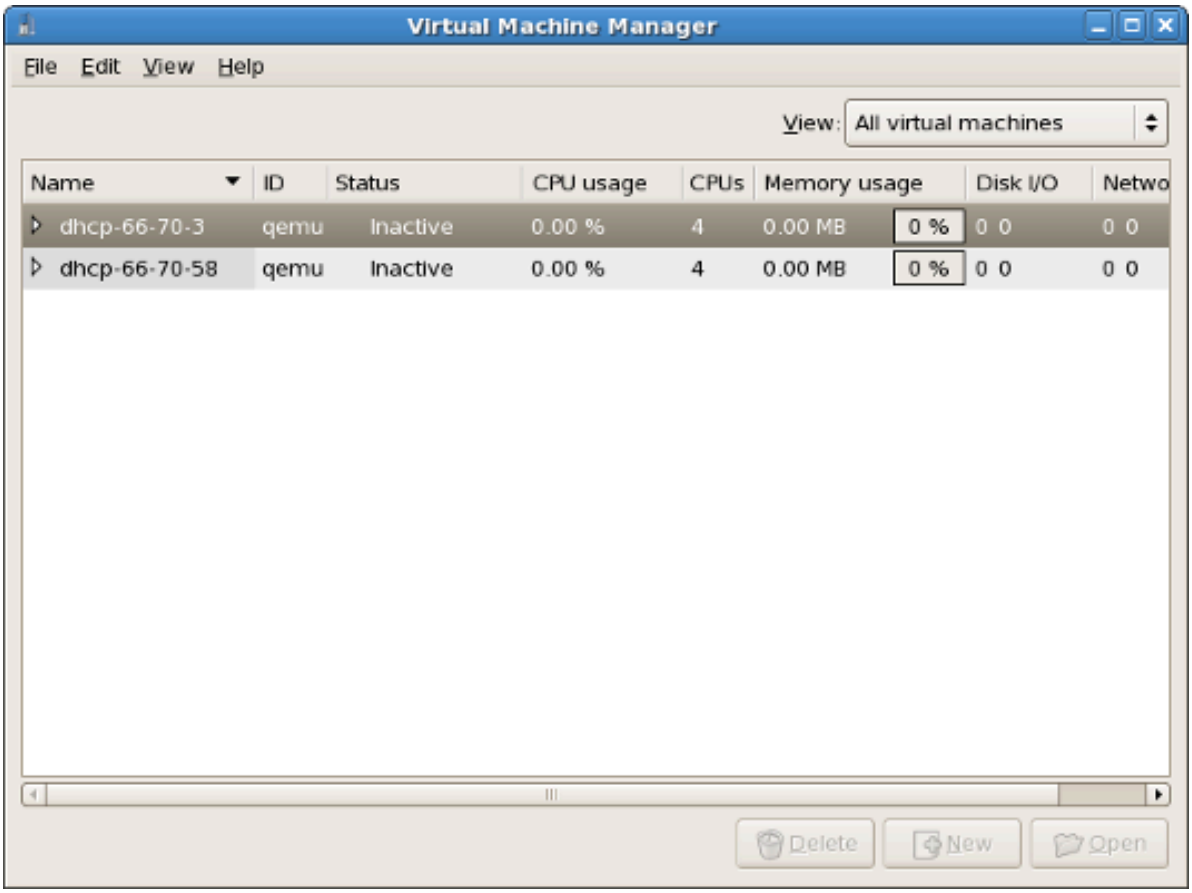
   Ingrese la siguiente información:

   - **Hipervisor**: Seleccionar **QEMU**.
   - **Conexión**: Seleccionar el tipo de conexión.
   - **Nombredehost**: Ingrese el nombre del host.

   Haga clic en **Conectar**.



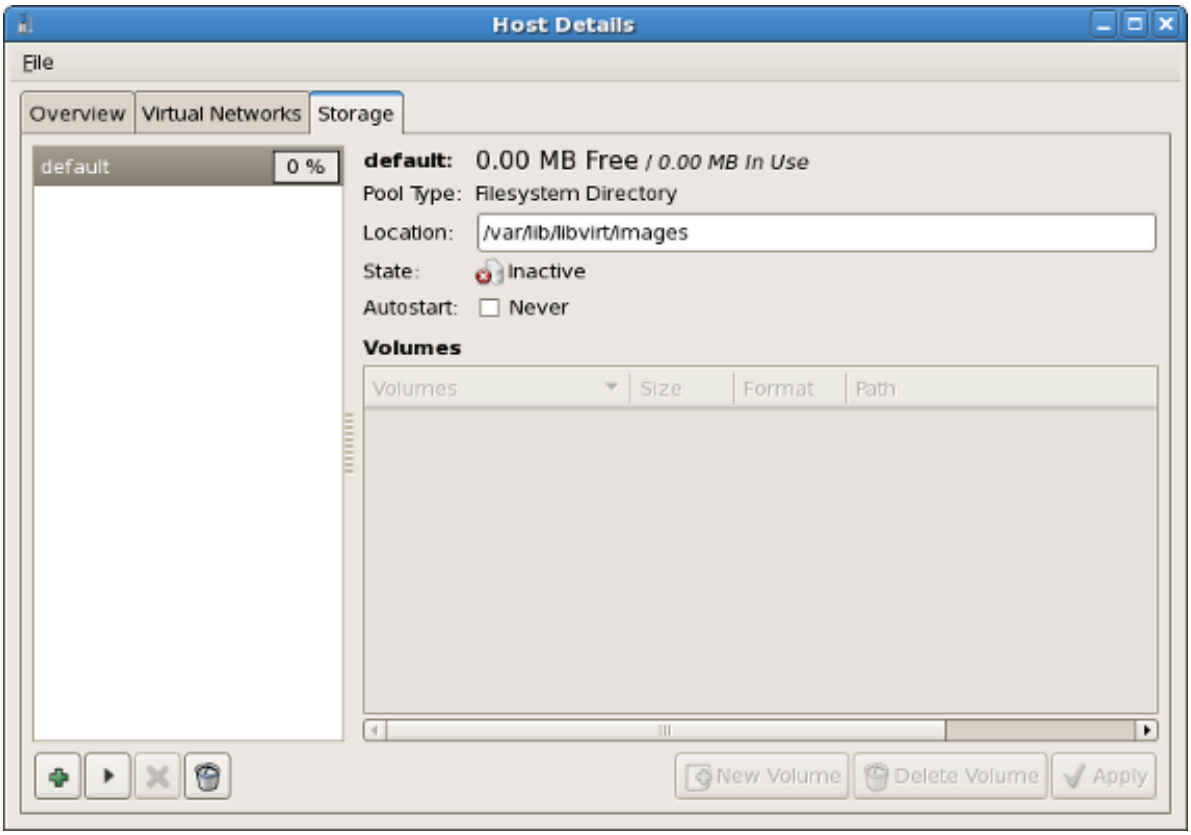
El administrador de la máquina virtual muestra una lista de los hosts conectados.


Virtual Machine Manager
File Edit View Help
View: All virtual machines
Name ID Status CPU usage CPUs Memory usage Disk I/O Netwo
dhcp-66-70-3 qemu Inactive 0.00 % 4 0.00 MB 0 % 0 0 0 0
dhcp-66-70-58 qemu Inactive 0.00 % 4 0.00 MB 0 % 0 0 0 0
Delete New Open

2. Agregar un grupo de almacenaje con el mismo NFS a la fuente y hosts de destino.

   En el menú **Editar**, haga clic en **Información de host**, la ventana de información de host aparecerá.

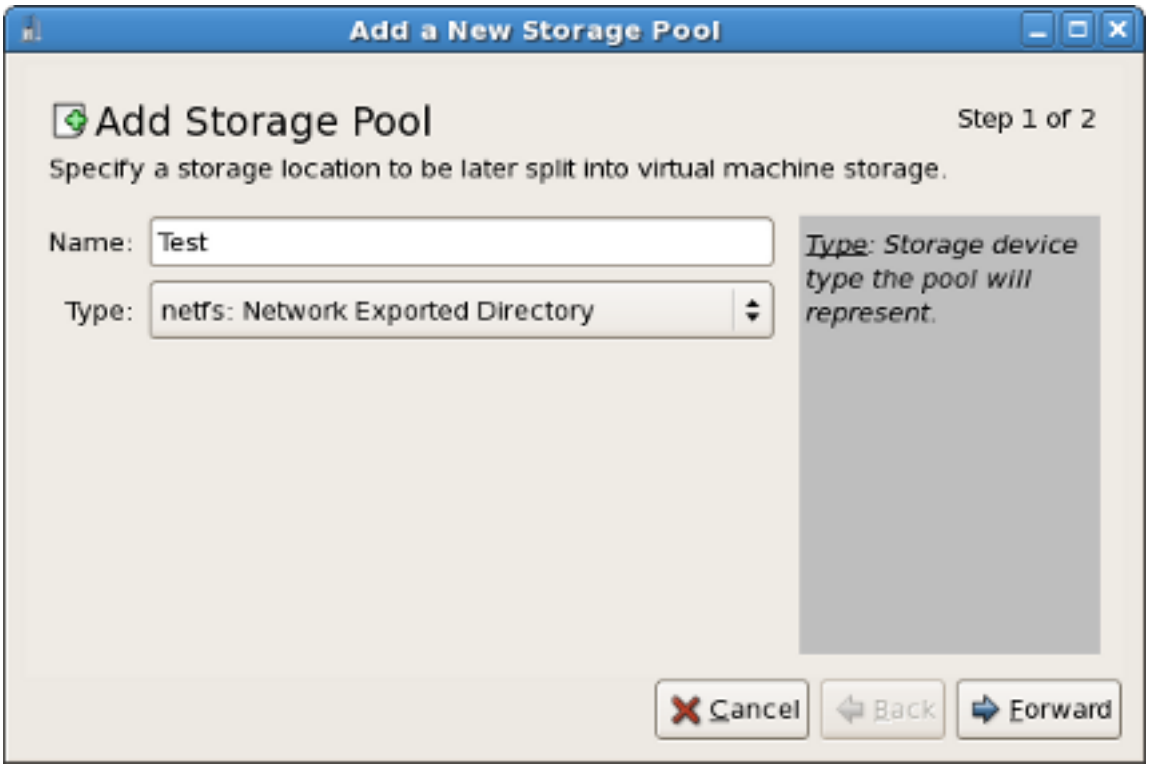
   Haga clic en la pestaña **Almacenaje**.



3. Agregar un nuevo grupo de almacenaje. En la esquina inferior izquierda de la ventana, haga clic en el botón **+**. La ventana de Agregar un nuevo grupo de almacenaje, aparecerá.

   Ingrese la siguiente información:

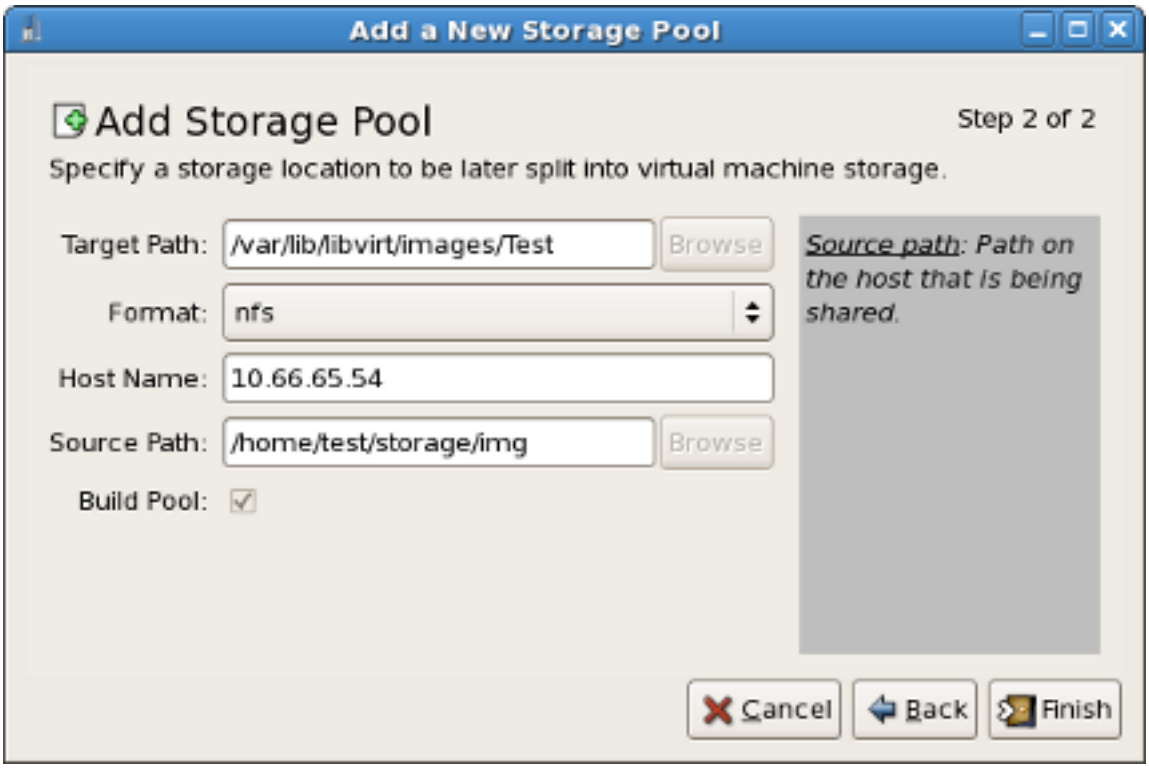
   - **Nombre**: Entrar el nombre del grupo de almacenaje.
   - **Tipo**: Seleccionar **netfs: Directorio de red exportado**.



Haga clic en **Adelante**.

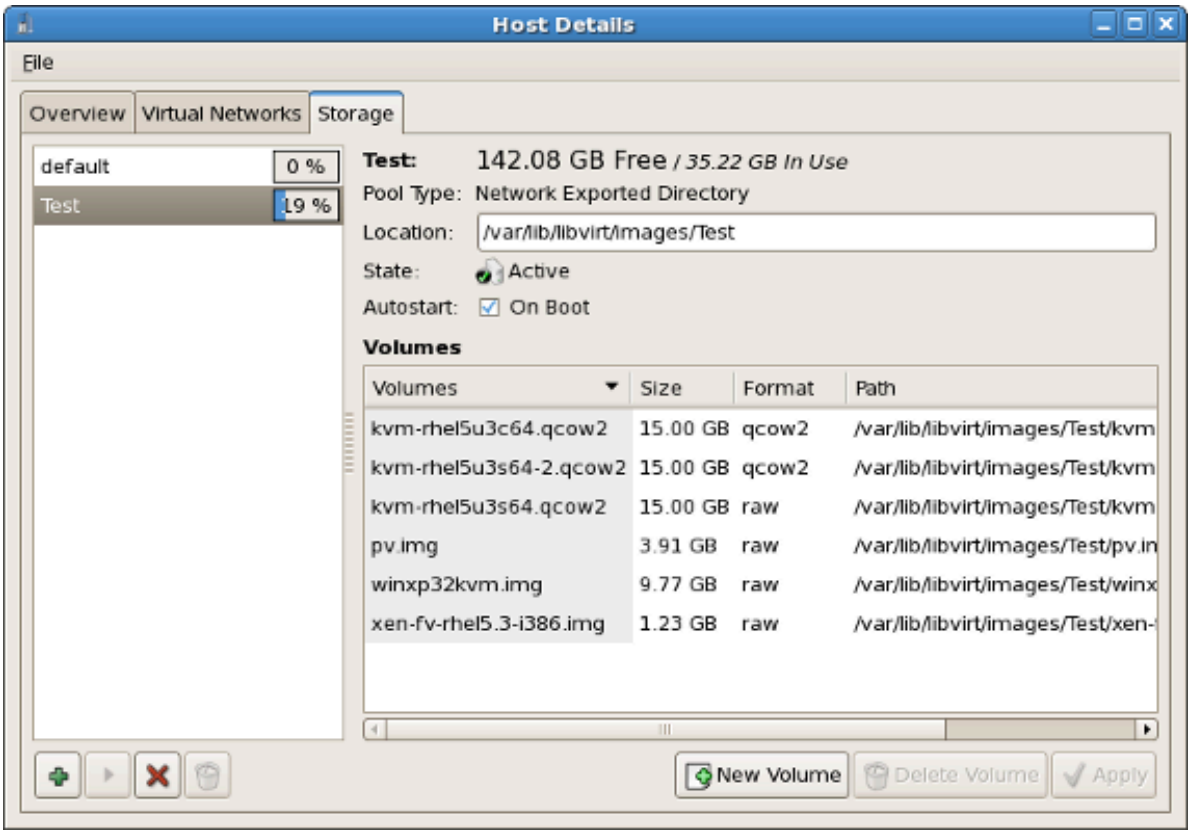
4. Ingrese la siguiente información:

   - **Formato**: Seleccione el tipo de almacenaje. Éste debe ser NFS o iSCSI para migraciones en vivo.
   - **Nombre de host**: Entra la dirección IP o el nombre de dominio totalmente cualificado del servidor de almacenaje.

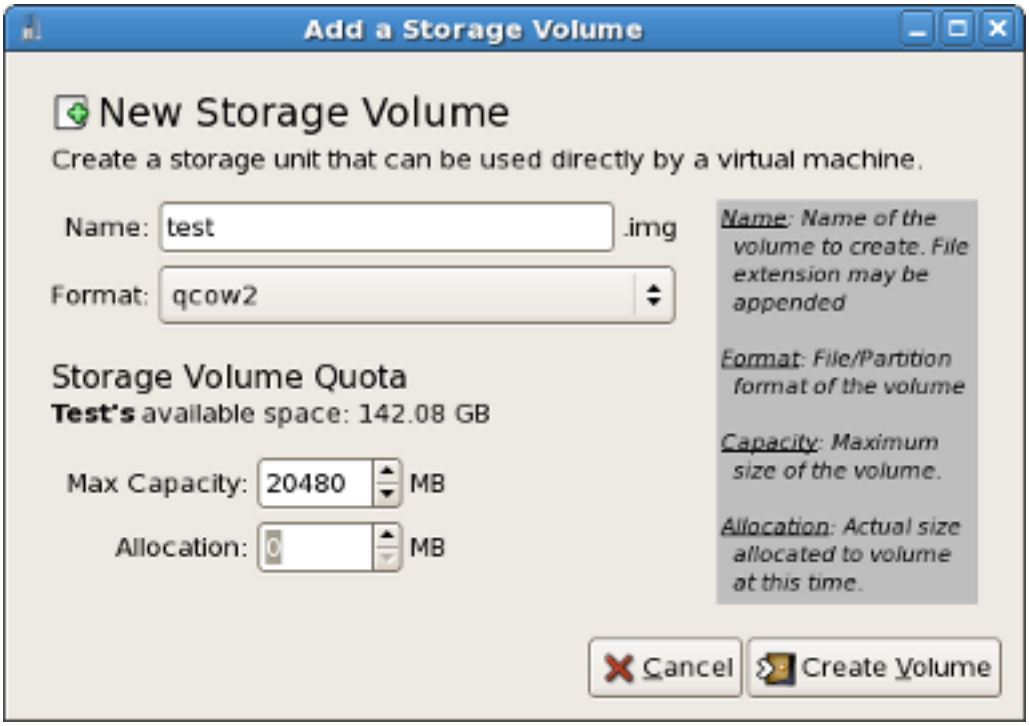


Haga clic en **Terminar**.

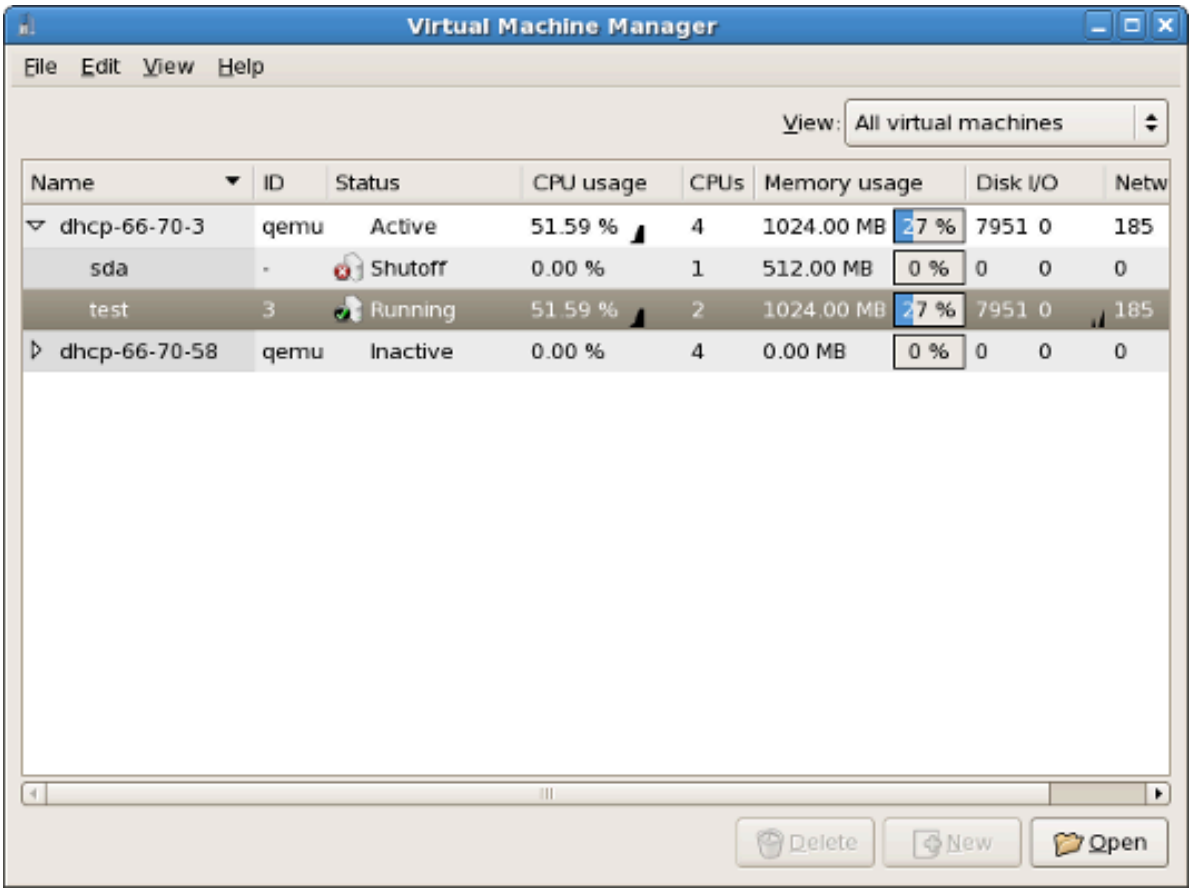
5. Cree un nuevo volumen en el grupo de almacenaje compartido, haga clic en **Nuevo volumen**.



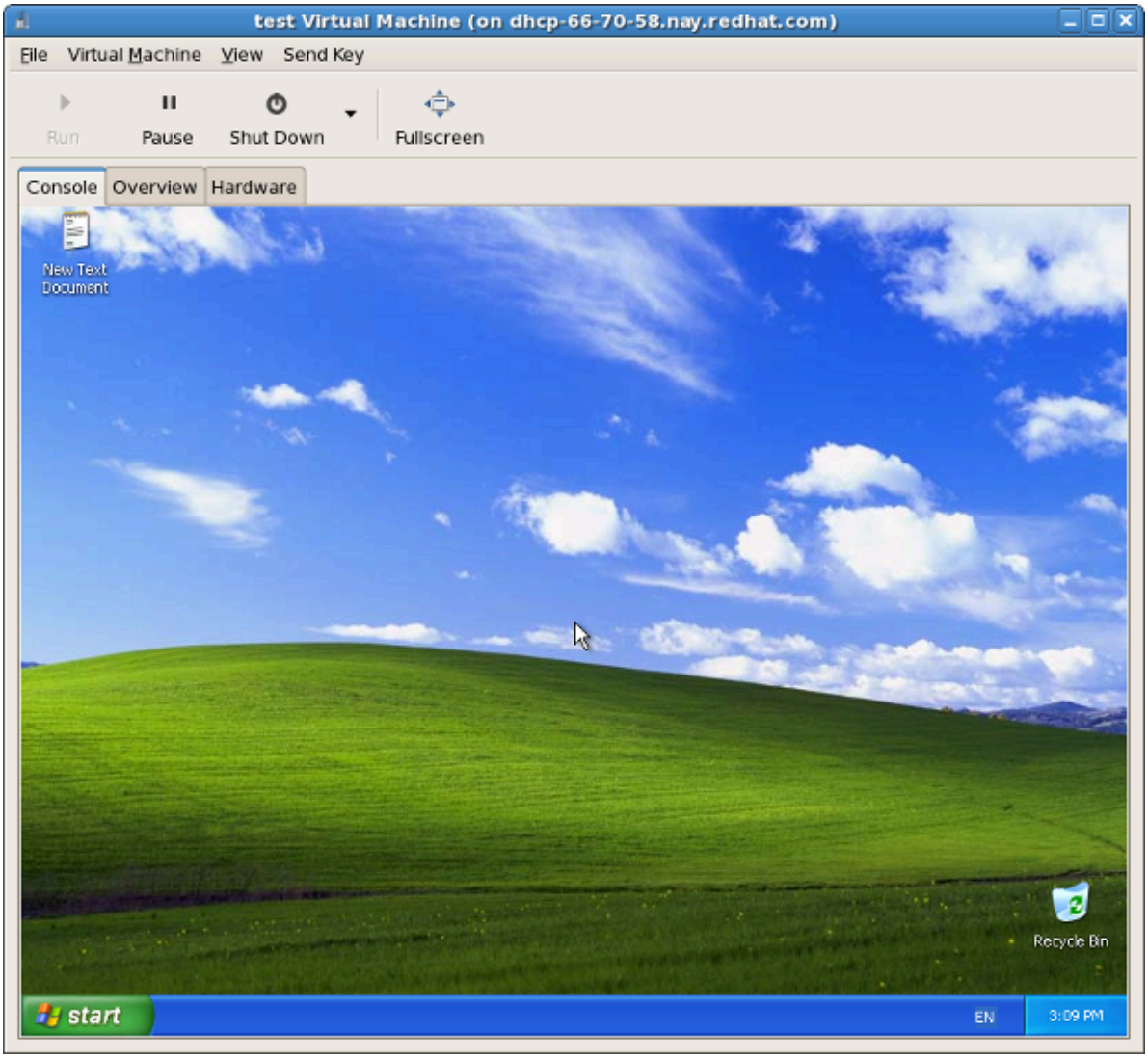
6. Ingrese los detalles, luego haga clic en **Crear volumen**.


Add a Storage Volume
New Storage Volume
Create a storage unit that can be used directly by a virtual machine.
Name: test .img
Format: qcow2
Storage Volume Quota
Test's available space: 142.08 GB
Max Capacity: 20480 MB
Allocation: 0 MB
Name: Name of the volume to create. File extension may be appended
Format: File/Partition format of the volume
Capacity: Maximum size of the volume.
Allocation: Actual size allocated to volume at this time.
Cancel
Create Volume

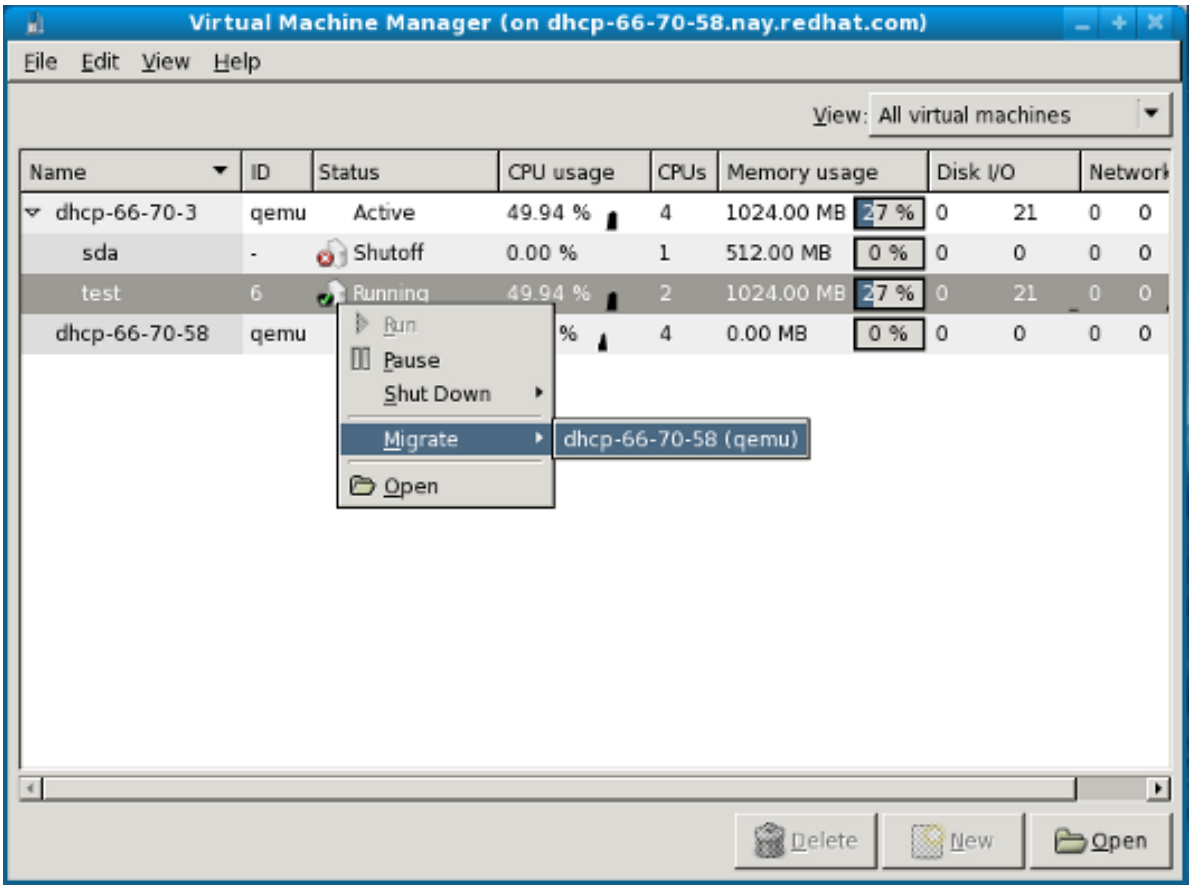
7. Cree una máquina virtual con el nuevo volumen, luego ejecute la máquina virtual.


Virtual Machine Manager
File Edit View Help
View: All virtual machines
Name ID Status CPU usage CPUs Memory usage Disk I/O Netw
dhcp-66-70-3 qemu Active 51.59 % 4 1024.00 MB 27 % 7951 0 185
sda - Shutoff 0.00 % 1 512.00 MB 0 % 0 0 0
test 3 Running 51.59 % 2 1024.00 MB 27 % 7951 0 185
dhcp-66-70-58 qemu Inactive 0.00 % 4 0.00 MB 0 % 0 0 0
Delete
New
Open

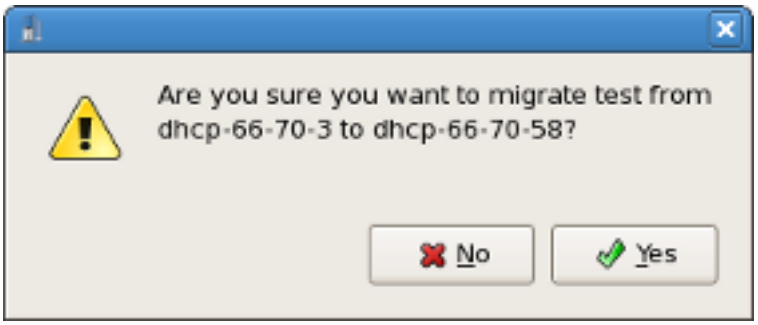
Aparecerá la Ventana de máquina virtual.



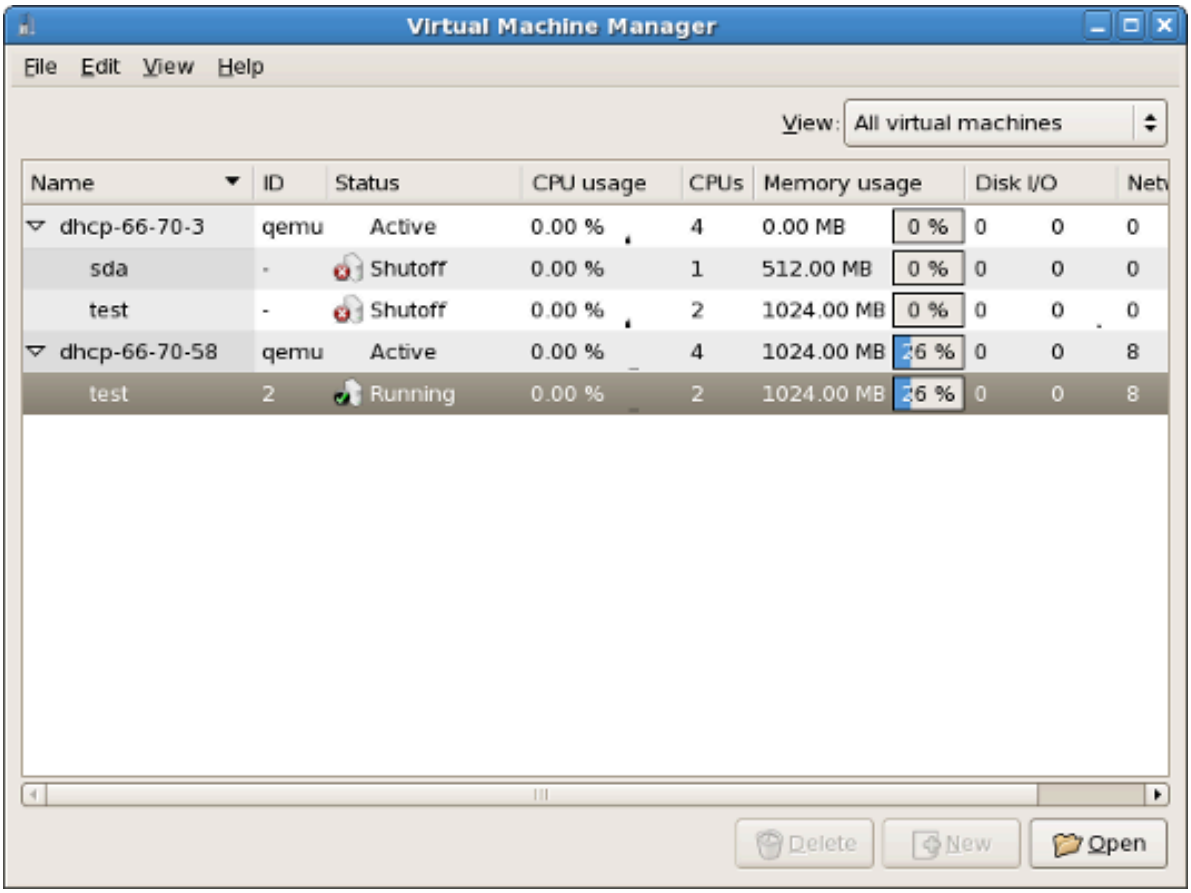
8. En la ventana de la máquina virtual, haga clic derecho en la máquina virtual, seleccione **Migrar**, luego haga clic en la ubicación de la migración.


Virtual Machine Manager (on dhcp-66-70-58.nay.redhat.com)
File Edit View Help
View: All virtual machines
Name ID Status CPU usage CPUs Memory usage Disk I/O Network
dhcp-66-70-3 qemu Active 49.94 % 4 1024.00 MB 27 % 0 21 0 0
sda - Shutoff 0.00 % 1 512.00 MB 0 % 0 0 0 0
test 6 Running 49.94 % 2 1024.00 MB 27 % 0 21 0 0
dhcp-66-70-58 qemu % 4 0.00 MB 0 % 0 0 0 0
Run
Pause
Shut Down
Migrate
dhcp-66-70-58 (qemu)
Open
Delete
New
Open

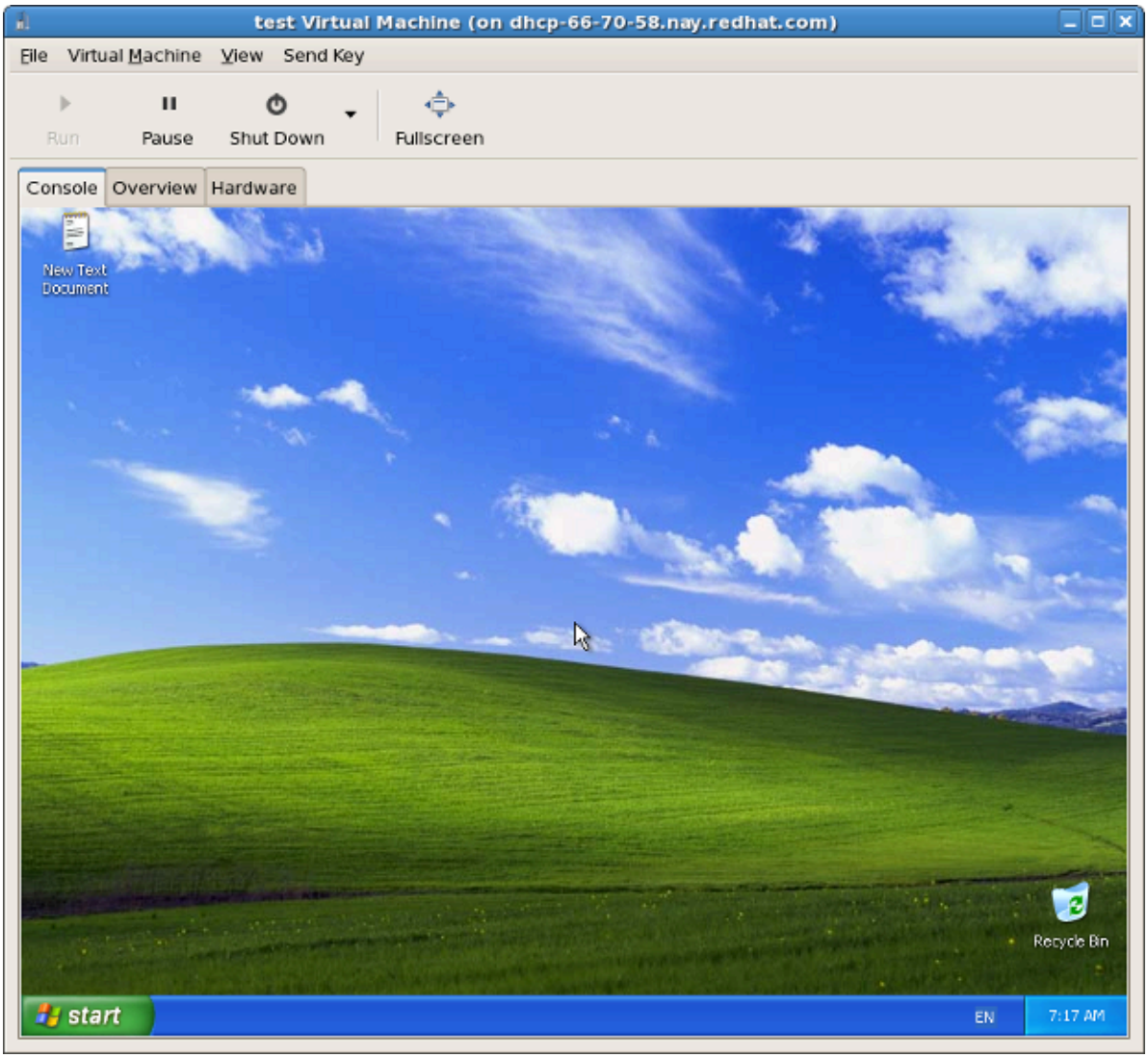
9. Haga clic en **Sí** para confirmar la migración.



El administrador de la Máquina virtual muestra la máquina virtual en su nueva ubicación.


Virtual Machine Manager
File Edit View Help
View: All virtual machines
Name ID Status CPU usage CPUs Memory usage Disk I/O Net
dhcp-66-70-3 qemu Active 0.00 % 4 0.00 MB 0 % 0 0 0
sda - Shutoff 0.00 % 1 512.00 MB 0 % 0 0 0
test - Shutoff 0.00 % 2 1024.00 MB 0 % 0 0 0
dhcp-66-70-58 qemu Active 0.00 % 4 1024.00 MB 6 % 0 0 8
test 2 Running 0.00 % 2 1024.00 MB 6 % 0 0 8
Delete New Open

The VNC connection displays the remote host's address in its title bar.


test Virtual Machine (on dhcp-66-70-58.nay.redhat.com)
File Virtual Machine View Send Key
Run
Pause
Shut Down
Fullscreen
Console Overview Hardware
New Text Document
Recycle Bin
start
EN
7:17 AM

Administración remota de huéspedes virtualizados

Esta sección explica cómo administrar de forma remota sus huéspedes virtualizados mediante **ssh** o TLS y SSL.

21.1. Administración remota con SSH

El paquete *ssh* proporciona un protocolo de red encriptado, el cual puede enviar funciones de administración seguras a servidores de virtualización remotos. El método descrito utiliza administración de conexión segura de **libvirt** en túnel en conexión **SSH** para administrar máquinas remotas. Toda la autenticación se realiza a través de la criptografía de llave pública **SSH** y contraseñas y frases de acceso reunidas por el agente local **SSH**. Además la consola **VNC** para cada máquina virtual de huésped es puesta en túnel a través de **SSH**.

SSH suele estar configurado por defecto, por lo tanto, probablemente ya tiene llaves SSH configuradas y no necesita reglas de firewall adicionales para acceder al servicio de administración o consola **VNC**.

Tenga presentes los problemas que se pueden presentar al usar **SSH** para manejar de forma remota sus máquinas virtuales, incluyendo:

- Se requiere registro de root para acceder a la máquina remota para máquinas virtuales,
- El proceso de configuración de conexión inicial puede ser lento,
- there is no standard or trivial way to revoke a user's key on all hosts or guests, and
- ssh no escala bien con grandes cantidades de máquinas remotas

Cómo configurar el acceso SSH de `virt-manager` sin contraseñas, o con contraseñas administradas

Las siguientes instrucciones presuponen que usted está iniciando el proceso desde el principio, y que no aún no ha definido ninguna llave **SSH**. Si ya posee llaves SSH y ya las ha copiado en otros sistemas, entonces puede saltearse este procedimiento.

El usuario es importante para administración remota

Las llaves SSH son dependientes del usuario. Solo el usuario que es dueño de una determinada llave puede acceder a ella.

El comando **virt-manager** debe ser ejecutado bajo el usuario que es dueño de las llaves para conectarse con el equipo remoto. Eso significa que, si los sistemas remotos están administrados por un usario diferente al usuario root, **virt-manager** debe ejecutarse si los privilegios del usuario root. Si el sistema remoto se encuentra administrado por el usuario root correspondiente, entonces las llaves SSH deben ser creadas y le deben pertenecer al usuario root.

Utilizando **virt-manager** no puede administrarse el equipo local como un usuario sin privilegios de root.

1. **Opcional: Utilizar otro usuario**
   Si es necesario, cambie de usuario. El siguiente ejemplo utiliza el usuario root local para administrar en forma remota al equipo local, y al resto de los equipos.

   ```
   $ su -
   ```

2. **Cómo generar el par de lleves SSH**
   Genere un par de llaves públicas en la máquina en donde está siendo utilizado **`virt-manager`**. El ejemplo siguiente utiliza la ubicación predeterminada de la llave, en el directorio **`~/.ssh/`**.

   ```
   $ ssh-keygen -t rsa
   ```

3. **Cómo copiar las llaves en los equipos remotos**
   El registro remoto sin una contraseña, o con una frase de acceso, necesita una llave SSH para ser distribuida en los sistemas que están siendo administrados. Utilice el comando ssh-copy-id para copiar la llave en el usuario root en la dirección del sistema ofrecida (en el ejemplo, *`root@example.com`*).

   ```
   # ssh-copy-id -i ~/.ssh/id_rsa.pub root@example.com root@example.com's password: Now
    try logging into the machine, with "ssh 'root@example.com'", and check in: .ssh/
   authorized_keys to make sure we haven't added extra keys that you weren't expecting
   ```

   De acuerdo a lo que necesite, repita este procedimiento en otros sistemas.

4. **Opcional: Agregue una frase de acceso al agente ssh**
   Si lo necesita, agregue la frase de acceso para la llave SSH a **`ssh-agent`**. En el equipo local, utilice el siguiente comando para agregar la frase de acceso (si es que hubiera alguna), para habilitar registros sin contraseñas.

   ```
   # ssh-add ~/.ssh/id_rsa.pub
   ```

La llave SSH fue agregada el sistema remoto.

El demonio `libvirt` (`libvirtd`)

El demonio `libvirt` proporciona una interfaz para administrar las máquinas virtuales. Debe tener este demonio instalado y en ejecución en cada equipo remoto que sea necesario administrar.

```
$ ssh root@somehost
# chkconfig libvirtd on
# service libvirtd start
```

Después de que `libvirtd` y **SSH** sean configurados, se debe poder acceder y administrar las máquinas virtuales de forma remota. También se podrá tener acceso a los huéspedes con **VNC** en este punto.

Cómo acceder a equipos remotos con virt.manager

Los equipos remotos pueden ser administraod con la herramienta gráfica de virt-manager. Las llaves SSH deben pertenecerle al usuario que se encuentre ejecutando virt-manager para que los registros sin contraseñas puedan funcionar.

1. Inicie virt-manager.
2. Open the **File**->**Add Connection** menu.
3. Input values for the hypervisor type, the connection, Connection->Remote tunnel over SSH, and enter the desired hostname, then click connection.

21.2. Administración remota en TLS y SSL

Puede administrar máquinas virtuales utilizando TLS y SSL. Ellos ofrecen un mejor escalamiento, pero su utilización es más complicada que ssh (consulte la *Sección 21.1, "Administración remota con SSH"*). TLS y SSL utilizan la misma tecnología que los navegadores de red para establecer conexiones seguras. El administrador de conexiones **`libvirt`** abre un puerto TCP para conexiones entrantes, el cual es cifrado y autenticado de modo seguro por certificados de tipo x509. Además, la consola de VNC para cada máquina huésped virtual será definida para utilizar TLS con autenticación de certificado x509.

This method does not require shell accounts on the remote machines being managed. However, extra firewall rules are needed to access the management service or VNC console. Certificate revocation lists can revoke users' access.

Pasos para configurar el acceso a TLS/SSL para virt-manager

La siguiente guía supone que se esta empezando de cero y que no se tiene conocimiento del certificado TLS/SSL. Si tiene la suerte de contar con un servidor de administración de certificado, probablemente puede pasar por alto estos pasos.

Configurar servidor de **`libvirt`**

Para mayor información sobre la creación de certificados, consulte **libvirt** en el sitio Web, *http://libvirt.org/remote.html*.

Configuración de cliente **`virt-manager`** y **`virsh`**

La configuración para cliente es un poco inconsistente en este momento. Para permitir la administración API de **`libvirt`** en TLS, los certificados CA y de cliente se deben ubicar en **`/etc/pki`**. Para mayor información, consulte *http://libvirt.org/remote.html*

In the **`virt-manager`** user interface, use the '**SSL/TLS**' transport mechanism option when connecting to a host.

Para **`virsh`**, el URI tiene el siguiente formato:

- **`qemu://hostname.guestname/system`** para KVM.

Para habilitar SSL y TLS para VNC, es necesario poner la autoridad de certificado y los certificados de cliente dentro de **`$HOME/.pki`**, es decir en los tres archivos siguientes:

- El certificado de CA - CA o **`ca-cert.pem`**.
- El certificado de cliente firmado por la CA - **`libvirt-vnc`** o **`clientcert.pem`**.
- La llave privada de cliente - **`libvirt-vnc`** o **`clientkey.pem`**.

21.3. Modos de transporte

Para administración remota, **`libvirt`** soporta los siguientes modos de transporte:

Seguridad de la capa de transporte, TLS (siglas en Inglés para Transport Layer Security)

La seguridad de capa de transporte TLS 1.0 (SSL 3.1) autenticada y el socket TCP/IP encriptado, generalmente escuchando en un número de puerto público. Para utilizarlo se necesitará generar certificados de cliente y servidor. El puerto estándar es 16514.

sockets de UNIX

Los sockets de dominio UNIX sólo se pueden acceder en la máquina local. Los sockets no están encriptados y utilizan permisos de UNIX o SELinux para autenticación. Los nombres de socket estándar son **`/var/run/libvirt/libvirt-sock`** y **`/var/run/libvirt/libvirt-sock-ro`** (para conexiones de sólo lectura).

SSH

Transportado sobre un protocolo de Shell seguro (SSH). Necesita que Netcat (el paquete *nc*) esté instalado. El demonio libvirt (**`libvirtd`**) debe estar ejecutándose en la máquina remota. El puerto 22 debe estar abierto para acceso de SSH. Se debe utilizar algún tipo de de administración de llave SSH (por ejemplo, la herramienta **`ssh-agent`**) o se le pedirá una contraseña.

ext

El parámetro *`ext`* es utilizado con cualquier programa externo que pueda realizar una conexión a una máquina remota por medios diferentes al ámbito de libvirt. Este parámetro se encuentra en una etapa de experimentación.

tcp

El socket TCP/IP sin encriptar. No se recomienda para uso de producción, por lo general está desactivado, pero un administrador lo puede habilitar para ensayarlo o utilizarlo en una red de confianza. El puerto predeterminado es 16509.

El transporte predeterminado es TLS, si no se especifica otro.

URI remotos

Un Identificador de recursos uniforme, URI (siglas en Ingles para Uniform Resource Identifier) es utilizado por **`virsh`** y **`libvirt`** para conectar a un host remoto. Los URI también se utilizan con el parámetro **`--connect`** para que el comando **`virsh`** ejecute comandos sencillos o migraciones en hosts remotos.

libvirt URIs take the general form (content in square brackets, "[]", represents optional functions):

```
driver[+transport]://[username@][hostname][:port]/[path][?extraparameters]
```

Se debe proporcionar ya sea el método de transporte o el nombre del equipo para identificar una ubicación externa.

Ejemplos de parámetros de administración remotos

- Se conecta con un equipo remoto KVM denominado `server7`, mediante la utilización tanto del transporte como del nombre de usuario SSH `ccurran`.

```
qemu+ssh://ccurran@server7/
```

- Se conecta con un hipervisor KVM remoto en el equipo denominado `server7` mediante TLS.

```
qemu://server7/
```

- Connect to a remote KVM hypervisor on host `server7` using TLS. The *`no_verify=1`* instructs libvirt not to verify the server's certificate.

```
qemu://server7/?no_verify=1
```

Prueba de ejemplos

- Conecta al hipervisor KVM local con un socket UNIX estándar. La ruta completa del socket de UNIX se proporciona explícitamente en este caso.

```
qemu+unix:///system?socket=/opt/libvirt/run/libvirt/libvirt-sock
```

- Conecte al demonio libvirt con una conexión encriptada de TCP/IP al servidor con la dirección IP 10.1.1.10 en puerto 5000. Éste utiliza el controlador de prueba con configuración predeterminada.

```
test+tcp://10.1.1.10:5000/default
```

Parámetros adicionales del URI

Pueden agregarse parámetros adicionales a URI remotos. La tabla que mostramos a continuación *Tabla 21.1, “Parámetros adicionales del URI”* describe los parámetros reconocidos. Cualquier otro tipo de parámetros es ignorado. Fíjese que los valores de los parámetros deben ser URI-escaped (es decir, se agrega un signo de interrogación (?) antes del parámetro y, los caracteres especiales son convertidos al formato de URI).

Nombre	Modo de transporte	Descripción	Uso de ejemplo
nombre	todos los modos	El nombre pasad o a la función remota virConnectOpen. El nombre se forma generalmente al eliminar transporte, nombre de host, número de puerto, nombre de usuario y parámetros adicionales desde el URI remoto, pero en algunos casos puede ser mejor proporcionar explícitamente el nombre.	name=qemu:///system

Nombre	Modo de transporte	Descripción	Uso de ejemplo
comando	ssh y ext	El comando externo. Para transporte ext este comando es requerido. Para ssh el predeterminado es ssh. La ruta es buscada por el comando.	command=/opt/openssh/bin/ssh
socket	unix y ssh	La ruta al socket de dominio de UNIX, la cual sobrescribe la predeterminada. Para transporte ssh, este pasa al comando netcat remoto (ver netcat).	socket=/opt/libvirt/run/libvirt/libvirt-sock
netcat	ssh	El comando **`netcat`** puede ser utilizado para conectarse a sistemas remotos. El parámetro netcat predeterminado utiliza el comando **nc**. Para transportes SSH, libvirt construye un comando SSH utilizando la forma que se muestra a continuación: *`command`* -p *`port`* [-l *`username`*] *`nombre del equipo`* *`netcat`* -U socket Los parámetros *`puerto`*, *`nombre de usuario`* y *`nombre equipo`* pueden especificarse como parte del URI remoto. Los parámetros *`command`*, *`netcat`* y *`socket`* provienen de otros parámetros externos.	netcat=/opt/netcat/bin/nc
no_verify	tls	If set to a non-zero value, this disables client checks of the server's certificate.	no_verify=1

Nombre	Modo de transporte	Descripción	Uso de ejemplo
		Note that to disable server checks of the client's certificate or IP address you must change the libvirtd configuration.	
no_tty	ssh	Si se establece a un valor de no-cero, ssh deja de pedir la contraseña si no puede ingresar automáticamente a una máquina remota (para usar el agente ssh o similar). Utilícelo cuando no tenga acceso a la terminal - por ejemplo, en programas gráficos que utilizan libvirt.	no_tty=1

Tabla 21.1. Parámetros adicionales del URI

KSM

El concepto de memoria compartida es común en los sistemas operativos modernos. Por ejemplo, cuando un programa es iniciado por primera vez el comparte la memoria con el programa padre. Cuando el programa padre o el hijo intenta modificar esta memoria, el núcleo asigna una nueva área de memoria, copia el contenido original a esta area y permite la modificación de esta área. Esto se conoce como copia en escritura.

KSM es una función nueva en Linux que usa este concepto en reversa. KSM permite al núcleo examinar dos o mas programas y comparar la memoria en uso. Si alguna región de memoria es idéntica, el núcleo puede combinar las dos áreas en una sola y marcar estas regiones como copia en escritura igual que en el ejemplo anterior.

Esto es de gran ayuda para la virtualisación con KVM. Cuando un huésped virtual inicia, el solo hereda la memoria del proceso padre `qemu-kvm`. Una vez el huésped esta corriendo la imagen del sistema operativo huésped puede ser compartida si el huésped usa el mismo sistema operativo o aplicación.

El beneficio de KSM es velocidad y utilidad. Con KSM, la data común se mantiene en la memoria principal o el cache. Esto reduce las faltas en el cache para los huéspedes KVM que pueden incrementar su desempeño para esas aplicaciones o sistemas operativos, el uso de memoria compartida reduce el consumo de memoria en los huéspedes y permite una cantidad mayor de huéspedes así como mejor uso de los recursos.

Activando KSM

Pendiente

Desactivando KSM

Pendiente

Ajustando KSM

Pendiente

Advanced virtualization administration

This chapter covers advanced administration tools for fine tuning and controlling virtualized guests and host system resources.

Nota

This chapter is a work in progress. Refer back to this document at a later date.

23.1. Guest scheduling

KVM guests function as Linux processes. By default, KVM guests are prioritised and scheduled with the Linux Completely Fair Scheduler. Tuning the schedule for guest processes may be required for some environments or to prioritize certain guests.

23.2. Advanced memory management

Capping memory available to guests and preventing overcommit on certain guests.

23.3. Guest block I/O throttling

Limit guest block I/O throughput.

23.4. Guest network I/O throttling

Limit guest network activity.

Migración de Xen a KVM

Ya no es posible.

24.1. Xen a KVM

Este capítulo cubre las migraciones de invitados Fedora con hipervisor Xen a Fedora con hipervisor KVM.

24.2. Versiones viejas de KVM a KVM

Este capítulo cubre las migraciones de invitados de Fedora con hipervisor KVM a Fedora con hipervisor KVM.

Tareas de administración diversas

El presente capítulo contiene trucos y consejos útiles para mejorar el desempeño, la adaptabilidad y la estabilidad de la virtualización.

25.1. Cómo iniciar los huéspedes automáticamente

This section covers how to make virtualized guests start automatically during the host system's boot phase.

Nuestros ejemplos utilizan **`virsh`** para definir un huésped, *`TestServer`* para iniciarlo cuando el equipo arranca.

```
# virsh autostart TestServer
Domain TestServer marked as autostarted
```

Ahora el huésped se inicia automáticamente junto con el equipo.

Para detener un huésped que se ha iniciado automáticamente en el arranque, utilice el parámetro `--disable`.

```
# virsh autostart --disable TestServer
Domain TestServer unmarked as autostarted
```

El huésped no se iniciará automáticamente con el equipo.

25.2. Cómo utilizar qemu-img

La herramienta de línea de comando **`qemu-img`** es utilizada para dar formato a numerosos sistemas de archivos utilizados por KVM. **`qemu-img`** debería utilizarse para formatear imágenes de huéspedes virtualizadas, dispositivos de almacenamiento adicionales y almacenamiento de red. A continuación ofrecemos una lista con las opciones y modos de utilización de **`qemu-img`**.

Cómo crear y darle formato a nuevas imágenes o dispositivos

Genere el nombre de archivo para la la nueva imagen de disco del tamaño *`size`* y con el formato *`format`*.

```
# qemu-img create [-6] [-e] [-b base_image] [-f format] filename [size]
```

If base_image is specified, then the image will record only the differences from base_image. No size needs to be specified in this case. base_image will never be modified unless you use the "commit" monitor command.

Convertir una imagen existente a un formato diferente

La opción *`convert`* es utilizada para convertir un formato reconocido a

Formato del comando:

```
# qemu-img convert [-c] [-e] [-f format] filename [-O output_format] output_filename
```

Convierta la imagen de disco *filename* existente a la nueva *output_filename* utilizando el formato *output_format*. De forma opcional, la imagen de disco puede cifrarse con la opción *-e*, o comprimirse con la opción *-c*.

Solo el formato **qcow** ofrece soporte para cifrado o compresión. La compresión ofrece solamente el modo lectura. Esto significa que si un sector comprimido es sobrescrito, entonces será sobrescrito como datos sin comprimir.

El cifrado utiliza el formato AES con llaves muy seguras de 128 bits. Utilice una contraseña extensa (más de 16 caracteres) para obtener la mayor protección.

La conversión de imágenes también es útil para obtener imágenes más pequeñas cuando se esté utilizando un formato que puede expandirse, como es por ejemplo **qcow** o **cow**. Los sectores vacíos son detectados y suprimidos de la imagen de destino.

Cómo obtener la información de la imagen

El parámetro **info** muestra información acerca de la imagen de disco. El formato para la opción **info** es el siguiente:

```
# qemu-img info [-f format] filename
```

Ofrece información acerca del archivo de la imagen de disco. Utilícelo especialmente para conocer el tamaño reservado en el disco, y que puede ser diferente que el del tamaño indicado. Si las capturas de MV son almacenados en la imagen del disco, ello también serán visualizados.

Formatos soporttados

El formato de una imagen, por lo general es adivinado de manera automática. Existe soporte para los siguientes formatos:

raw
: Formato de imagen de disco raw (predeterminado). Este formato posee la ventaja de ser sencillo y fácilmente exportable hacia el resto de los emuladores. Si su sistema de archivos soporta huecos (por ejemplo ext2 o ext3 en LInux, o NTFS en Windows), entonces sólo los sectores escritos podrán reservar espacio. Utilice el comando **qemu-img info** para conocer el tamaño real utilizado por la imagen, o **ls -ls** en Unix/Linux.

qcow2
: El formato más versátil, el formato de imagen QEMU. Utilícelo para poseer imágenes más pequeñas (muy útil si su sistema de archivos no ofrece soporte para huecos, por ejemplo, con algunas versiones de Windows). De manera opcional ofrece cifrado AES, compresión basada en zlib, y soporte de numerosas capturas de MV.

qcow
: Antiguo formato de imagen QEMU. Sólo se ofrece por cuestiones de compatibilidad con versiones anteriores.

cow
: Formato de imagen del modo de usuario Linux "Copy on Write". El formato **cow** se ofrece sólo por cuestiones de compatibilidad con versiones anteriores. No funciona con Windows.

vmdk
: Formato de imagen compatible con VMware 3 y 4.

`cloop`
: Linux Compressed Loop image, útil solo para reutilizar directamente imágenes de CD-ROM comprimidas, como por ejemplo las que se utilizan en los CD-ROMs de la distribución Knoppix.

25.3. Sobrealojamiento con KVM

El hipervisor de KVM ofrece soporte para sobrealojar CPUs y memoria. Se denomina sobrealojamiento al hecho de alojar más CPUs virtualizadases, o más memoria, que la que exista físicamente en los recursos del sistema. Con un sobrealojamiento de CPUs, los servidores o sistemas de escritorio que no se estén utilizando podrán ejecutarse sobre menor cantidad de servidores, ahorrando así dinero y energía.

Cómo sobrealojar memoria

La mayoría de las aplicaciones y de los sistemas operativos no utilizan permanentemente el 100 % de la memoria RAM disponible. Esta conducta puede aprovecharse con KVM para que utilice más memoria de la que dispone físicamente para los huéspedes virtualizados.

Con KVM, las máquinas virtuales son procesos Linux. Los huéspedes en el hipervisor KVM no poseen bloques de memoria física RAM asignados, y en su lugar, funcionan como procesos. Cada proceso aloja memoria en la medida que la necesite. KVM utiliza esta característica para poder alojar la memoria que necesiten los huéspedes, en la medida que el sus sistemas operativos así lo requieran. El huésped utilizará solo un poco más de la memoria física que el sistema operativo virtualizado.

When physical memory is nearly completely used or a process is inactive for some time, Linux moves the process's memory to swap. Swap is usually a partition on a hard disk drive or solid state drive which Linux uses to extend virtual memory. Swap is significantly slower than RAM.

Como las máquinas virtuales KVM son procesos Linux, la memoria utilizada por los huéspedes virtualizados puede ser colocada en swap, en caso que el huésped se encuentre inactivo, o sin una utilización importante. La memoria puede ser alojada superando el tamaño total de la memoria RAM física, o el espacio swap. Esto puede provocar inconvenientes si los huéspedes virtualizados utilizan la totalidad de la memorira RAM que se les ha asignado. Si no existe disponible suficiente espacio swap que permita que los procesos virtuales puedan ser "swapeados", se inicia **`pdflush`**, el proceso de limipieza. **`pdflush`** finaliza procesos de modo de poder liberar la menoria, evitando así una caída del sistema. **`pdflush`** podría destruir huéspedes virtualizados u otros sistemas operativos, y esto podría generar errores en el sistema de archivos, y hacer que algunos huéspedes no puedan volver a iniciarse.

Advertencia

Si no existe disponible suficiente swap, el sistema operativo huésped se apagará de manera forzada. Esto podría dejar a los huéspedes inoperables. Esto puede evitarlo si se cuida de no sobrealojar mayor cantidad de memoria que la cantidad disponible de espacio swap.

La partición swap es utilizada para "swapear" al disco rígido memoria sin utilizar de modo de poder acelerar el desempeño de la memoria. El tamaño predeterminado de la partición swap es calculado con la cantidad de memoria RAM y la tasa de sobrealojamiento. Si tiene intenciones de sobrealojar memoria con KVM, es recomendable generar una partición swap mayor para su sistema. Una tasa de sobrealojamiento recomendada es del 50% (0.5). La fótmula utilizada es la siguiente:

```
(0.5 * RAM) + (overcommit ratio * RAM) = Recommended swap size
```

El *Centro de documentación*[1] de Red Hat posee un artículo relacionado con la manera de poder determinar segura y eficientemente el tamaño de la partición swap.

Es posible ejecutar un sistema con una tasa de sobrealojamiento que, con respecto a la cantidad de memoria RAM física presente, sea diez veces mayor que la cantidad de huéspedes virtualizados. Esto solo funciona con la carga de determinadas aplicaciones (por ejemplo, virtualizaciones de escritorio que no estén utilizándose al 100%). La fórmula para poder configurar tasas de sobrealojamiento no es complicada, pero debe probarla y personalizarla de acuerdo a su entorno.

Cómo sobrealojar CPUs virtualizados

El hipervisor KVM ofrece soporte para sobrealojar CPUs virtualizados. Pueden sobrealojarse tanto como lo permitan los límites de carga de los huéspedes virtualizados. Sea cauteloso cuando realice sobrealojamientos de CPUs virtualizados, ya que las cargas cercanas al 100% del límite pueden provocar peticiones de desconexión, o tiempos de respuesta inutilizables.

El sobrealojamiento de CPUs virtualizados se realiza mejor cuando cada uno de los huéspedes virtualizados posee solo un CPU virtualizado. El planificador de Linux es muy eficiente con este tipo de carga. KVM debería soportar de manera segura a huéspedes con cargas menores al 100%, con una tasa de hasta cinco CPUs virtualizados. Sobrealojar un huésped virtualizado de un solo CPU virtualizado no es un problema.

No es posible sobrealojar huéspedes de multiprocesadores simétricos cuya cantidad de CPUs sea mayor a la de los núcleos de procesamiento físicos del sistema. Por ejemplo, un huésped con cuatro CPUs virtualizados no debería ser ejecutado en un equipo con un procesador de núcleo doble. Sobrealojar huéspedes de multiprocesadores simétricos en estas condiciones provocará una notable disminución en el desempeño de todo el sistema.

Asignar la misma cantidad de CPUs de huéspedes virtualizados que la de los núcleos de procesamiento físicos del sistema es adecuado y funciona perfectamente. Por ejemplo, ejecutar huéspedes virtualizados con cuatro CPUs virtualizados sobre un equipo con un procesador de cuatro núcleos. Los huéspedes con menos del 100% de carga deberían funcionar eficientemente en este esquema de configuración.

Primero realice pruebas, siempre

No sobrealoje memoria o CPUs en un entorno de producción, sin haber realizado primero las verificaciones adecuadas. Las aplicaciones que utilizan el 100% de la memoria o de los recursos de procesamiento, podrían tornarse inestables en entornos sobrealojados. Verifique antes de implementar.

25.4. Cómo verificar las extensiones de virtualización

Utilice esta sección para determinar si su sistema posee o no las extensiones de virtualización de hardware. Estas extensiones (Intel VT o AMD-V) son necesarias para una virtualización completa.

1. Ejecute el siguiente comando para verificar que se encuentren disponibles las extensiones de virtualización:

[1] http://kbase.redhat.com/faq/docs/DOC-15252

```
$ grep -E 'svm|vmx' /proc/cpuinfo
```

2. Analice el resultado.

   - El siguiente resultado contiene una entrada **vmx** indicando la existencia de un procesador Intel con las extensiones VT:

     ```
     flags   : fpu tsc msr pae mce cx8 apic mtrr mca cmov pat pse36 clflush
      dts acpi mmx fxsr sse sse2 ss ht  tm syscall lm constant_tsc pni monitor ds_cpl
      vmx est tm2 cx16 xtpr lahf_lm
     ```

   - El siguiente resultado contiene una entrada **svm** indicando la existencia de un procesador AMD con las extensiones AMD-V:

     ```
     flags   :  fpu tsc msr pae mce cx8 apic mtrr mca cmov pat pse36 clflush
      mmx fxsr sse sse2 ht syscall nx mmxext fxsr_opt lm 3dnowext 3dnow pni cx16
      lahf_lm cmp_legacy svm cr8legacy ts fid vid ttp tm stc
     ```

   Si cualquiera de estos resultados es el que ha obtenido, el procesador posee las extensiones de virtualización de hardware. Sin embargo, en algunas circunstancias, los fabricantes deshabilitan estas extensiones en el BIOS.

   The "**flags:**" output content may appear multiple times, once for each hyperthread, core or CPU on the system.

   Las extensiones de virtualización podrían estar deshabilitadas en el BIOS. Si las extensiones no aparecen, o una virtualización completa no funciona, diríjase a *Procedimiento 32.1, “Habilitar extensiones de virtualización en BIOS”*.

3. **Para usuarios del hipervisor KVM**
   Si el paquete kvm se encuentra instalado, como una verificación adicional, compruebe que los módulos **kvm** se encuentran cargados en el kernel:

   ```
   # lsmod | grep kvm
   ```

   Si el resultado incluye **kvm_intel** o **kvm_amd**, entonces los módulos **kvm** de virtualización de hardware se encuentran cargados, y su sistema cumple los requerimientos necesarios.

Resultados adicionales

Si el paquete *libvirt* ha sido instalado, el comando **virsh** puede ofrecer un resultado con la lista completa de capacidades de virtualización del sistema. Ejecute el comando **virsh capabilies** como usuario root para conocerla.

25.5. Cómo acceder a los datos desde una imagen de huésped de disco

Existen numerosos métodos para acceder a los datos desde archivos de imagen de huésped. Uno muy conocido es el de utilizar la herramienta **kpartx**, descrita en esta sección, de modo de poder montar el sistema de archivos huésped comu un dispositivo de bucle al que puede accederse.

El comando **kpartx** genera mapeos de dispositivos desde tablas de partición. Cada imagen de almacenamiento de huésped posee una tabla de partición incrustada en el archivo.

Los paquetes *libguestfs* y *guestfish*, disponibles en el repositorio *EPEL*[2], permiten modificaciones avanzadas y acceso a los sistema de archivos del huésped. Los paquetes *libguestfs* y *guestfish* no son descritos en esta sección.

Advertencia

Los huéspedes deben estar desconectados antes que sus archivos puedan ser leídos. No es posible ni editar ni leer los archivos de un huésped activo, e intentarlo podría causar pérdida de datos o daños.

Procedimiento 25.1. Cómo acceder a los datos de la imagen del huésped

1. Instale el paquete *kpartx*.

```
# yum install kpartx
```

2. Utilice kpartx para conocer los mapeos de los dispositivos de particionamiento asociados a una imagen de almacenamiento basada en archivo. El siguiente ejemplo utiliza un archivo de imagen denominado *guest1.img*.

```
# kpartx -l /var/lib/libvirt/images/guest1.img
loop0p1 : 0 409600 /dev/loop0 63
loop0p2 : 0 10064717 /dev/loop0 409663
```

   guest1 es un huésped Linux. La primer partición es la partición de arranque, y la segunda es de formato EXT3 y es la partición raíz (root).

3. Agregue los mapeos de partición a los dispositivos reconocidos en **/dev/mapper/**.

```
# kpartx -a /var/lib/libvirt/images/guest1.img
```

   - Verifique que funcione el mapeo de las particiones. Deberían existir nuevos dispositivos en el directorio /dev/mapper/.

```
# ls /dev/mapper/
loop0p1
loop0p2
```

     Los mapeos para la imagen son denominados con el formato **loopXpY**.

[2] http://fedoraproject.org/wiki/EPEL

4. Monte el dispositivo de bucle en un directorio. Si es necesario, genere el directorio. El ejemplo que damos a continuación utiliza al directorio **/mnt/guest1** para montar la partición.

```
# mkdir /mnt/guest1
# mount /dev/mapper/loop0p1 /mnt/guest1 -o loop,ro
```

5. Los archivos ahora se encuentran disponibles para ser leídos en el directorio **/mnt/guest1**. Léalos, o cópielos.

6. Desmonte el dispositivo de manera que la imagen de huésped pueda ser reutilizada por él. Si el dispositivo se encuentra montado, el huésped no podrá acceder a la imagen, y por lo tanto, no podrá iniciarse.

```
# umount /mnt/tmp
```

7. Desconecte el archivo de imagen de los mapeos de partición.

```
# kpartx -d /var/lib/libvirt/images/guest1.img
```

Ahora el huésped puede ser reiniciado.

Cómo acceder a los datos desde volúmenes de huéspedes LVM

Numerosos huéspedes Linux utilizan volúmenes de Logical Volume Management (LVM). Se necesitan algunos pasos adicionales para leer datos de volúmenes LVM de imágenes de almacenamiento virtual.

1. Agregue los mapeos de partición para el *guest1.img* a los dispositivos reconocidos en el directorio **/dev/mapper/**.

```
# kpartx -a /var/lib/libvirt/images/guest1.img
```

2. En nuestro ejemplo, los volúmenes LVM se encuentran en una segunda partición. Los volúmenes necesitan de otro análisis con el comando **vgscan**, para que pueda encontrar los nuevos grupos de volúmenes.

```
# vgscan
Reading all physical volumes . This may take a while...
Found volume group "VolGroup00" using metadata type lvm2
```

3. Active el grupo de volúmenes en la partición (denominada **VolGroup00** por defecto), con el comando **vgchange -ay**.

```
# vgchange -ay VolGroup00
2 logical volumes in volume group VolGroup00 now active.
```

4. Utilice el comando **lvs** para observar información relacionada con los nuevos volúmenes. Los nombres de estos volúmenes (la columna **LV**) son necesarios para poder montarlos.

```
# lvs
LV VG Attr Lsize Origin Snap% Move Log Copy%
LogVol00 VolGroup00 -wi-a- 5.06G
```

```
LogVol01 VolGroup00 -wi-a- 800.00M
```

5. Monte el volumen **/dev/VolGroup00/LogVol00** en el directorio **/mnt/guestboot/**.

```
# mount /dev/VolGroup00/LogVol00 /mnt/guestboot
```

6. Ahora los archivos se encuentran disponibles para ser leídos en el directorio **/mnt/guestboot**. Léalos o cópielos.

7. Desmonte el dispositivo de manera que la imagen de huésped pueda ser reutilizada por él. Si el dispositivo se encuentra montado, el huésped no podrá acceder a la imagen, y por lo tanto, no podrá iniciarse.

```
# umount /mnt/
```

8. Desconecte el grupo de volúmenes *VolGroup00*

```
# vgchange -an VolGroup00
```

9. Desconecte el archivo de imagen de los mapeos de partición.

```
# kpartx -d /var/lib/libvirt/images/guest1.img
```

Ahora el huésped puede ser reiniciado.

25.6. Cómo configurar las afinidades de un procesador KVM

Esta sección describe la configuración de las afinidades del núcleo del procesador, y del procesador en sí, mediante **libvirt** sobre huéspedes KVM.

By default, libvirt provisions guests using the hypervisor's default policy. For most hypervisors, the policy is to run guests on any available processing core or CPU. There are times when an explicit policy may be better, in particular for systems with a NUMA (Non-Uniform Memory Access) architecture. A guest on a NUMA system should be pinned to a processing core so that its memory allocations are always local to the node it is running on. This avoids cross-node memory transports which have less bandwidth and can significantly degrade performance.

En sistemas que no sean NUMA, podrían ser más eficientes determinadas formas de ubicación explicita entre los zócalos, núcleos, e hyperthreads de los equipos.

Cómo identificar la topología del CPU y de NUMA

El primer paso para poder decidir qué política aplicar, es determinar la memoria del equipo anfitrión y la topología de la CPU. El comando **virsh nodeinfo** ofrece información acerca de numerosos zócalos, núcleos e hyperthreads que se encuentran asociados al equipo

```
# virsh nodeinfo
CPU model:           x86_64
CPU(s):              8
CPU frequency:       1000 MHz
```

```
CPU socket(s):       2
Core(s) per socket:  4
Thread(s) per core:  1
NUMA cell(s):        1
Memory size:         8179176 kB
```

Este sistema posee ocho CPUs distribuidos en dos zócalos, y cada procesador tiene cuatro núcleos.

La salida muestra que el sistema posee una arquitectura NUMA. NUMA es más complejo y necesita más datos para interpretar adecuadamente. Utilice el comando **`virsh capabilities`** para obtener en la salida información adicional acerca de la configuración del CPU.

```
# virsh capabilities
<capabilities>
  <host>
    <cpu>
      <arch>x86_64</arch>
    </cpu>
    <migration_features>
      <live/>
      <uri_transports>
        <uri_transport>tcp</uri_transport>
      </uri_transports>
    </migration_features>
    <topology>
      <cells num='2'>
        <cell id='0'>
          <cpus num='4'>
            <cpu id='0'/>
            <cpu id='1'/>
            <cpu id='2'/>
            <cpu id='3'/>
          </cpus>
        </cell>
        <cell id='1'>
          <cpus num='4'>
            <cpu id='4'/>
            <cpu id='5'/>
            <cpu id='6'/>
            <cpu id='7'/>
          </cpus>
        </cell>
      </cells>
    </topology>
    <secmodel>
      <model>selinux</model>
      <doi>0</doi>
    </secmodel>
  </host>

 [ Additional XML removed ]

</capabilities>
```

La salida muestra dos nodos NUMA (también denominadas celdas NUMA), cada un conteniendo cuatro CPUs lógicos (cuatro núcleos de procesamiento). Este sistema posee dos zócalos, por lo tanto, podemos inferir que cada zócalo es un nodo NUMA diferente. Para un huésped con cuatro CPUs virtuales, lo ideal sería bloquearlo para que utilice de 0 a 3 CPUs físicas, o de 4 a 7 para evitar el acceso a memoria no local, ya que de hacer esto en lugar de utilizar memoria local, lo haría notoriamente más lento.

Si un huésped necesita ocho CPUs virtuales, ya que cada nodo NUMA solo posee cuatro CPUs físicas, una mejor utilización podría obtenerse ejecutando un par huéspedes con cuatro CPUs virtuales, dividiendo el trabajo entre ellos, en lugar de utilizar sólo uno con 8 CPUs. Una ejecución sobre varios nodos NUMA disminuye notoriamente el desempeño de las tareas, tanto físicas como virtuales.

Decida qué nodos NUMA pueden ejecutar el huésped

Bloquear un huésped para que utilice un nodo NUMA determinado no representa ningún beneficio si ese nodo no posee la memoria libre necesaria para ese huésped. Libvirt almacena información sobre la memoria libre disponible en cada nodo. Utilice el comando **`virsh freecell`** para conocer la memoria libre disponible en todos los nodos NUMA.

```
# virsh freecell
0: 2203620 kB
1: 3354784 kB
```

Si un huésped necesita el alojamiento de 3 GB de memoria RAM, entonces el huésped debería ejecutarse en un nodo (celda) NUMA 1. El nodo 0 sólo posee libres 2.2 GB, lo que probablemente no sea suficiente para determinados huéspedes.

Bloquee un huésped para que utilice un nodo NUMA, o un conjunto de CPU físico

Una vez que haya determinado sobre qué nodo ejecutar el huésped, conozca los datos de las capacidades (la salida del comando **`virsh capabilities`**) acerca de la tecnología NUMA.

1. Sección de la salida del comando **`virsh capabilities`**.

```
<topology>
  <cells num='2'>
    <cell id='0'>
    <cpus num='4'>
      <cpu id='0'/>
      <cpu id='1'/>
      <cpu id='2'/>
      <cpu id='3'/>
    </cpus>
  </cell>
  <cell id='1'>
    <cpus num='4'>
      <cpu id='4'/>
      <cpu id='5'/>
      <cpu id='6'/>
      <cpu id='7'/>
    </cpus>
  </cell>
  </cells>
</topology>
```

2. Observe that the node 1, **`<cell id='1'>`**, has physical CPUs 4 to 7.

3. El huésped puede ser bloqueado a un conjunto de CPUs agregándole el atributo **`cpuset`** al archivo de configuración.

    a. Si bien el huésped se encuentra desconectado, abra el archivo de configuración con el comando **`virsh edit`**.

b. Locate where the guest's virtual CPU count is specified. Find the **vcpus** element.

```
<vcpus>4</vcpus>
```

El huésped de nuestro ejemplo posee cuatro CPUs.

c. Agregue el atributo **cpuset** con los números de CPU para la celda NUMA pertinente.

```
<vcpus cpuset='4-7'>4</vcpus>
```

4. Guarde el archivo de configuración y reinicie el huésped.

El huésped ha sido bloqueado para que utilice los CPUs 4 a 7.

Bloquear automáticamente los huéspedes mediante virt-install para que utilicen determinados CPUs.

The **virt-install** provisioning tool provides a simple way to automatically apply a 'best fit' NUMA policy when guests are created.

La opción *cpuset* del comando **virt-install** puede utilizar un conjunto de procesadores de CPU, o el parámetro *auto*. Este último parámetro determina de manera automática el bloqueo ideal de CPUs, utilizando los datos NUMA disponibles.

Para un sistema NUMA, utilice el parámetro *--cpuset=auto* con el comando **virt-install** cuando sean creados huéspedes nuevos.

Cómo precisar afinidad CPU en huéspedes que se encuentren en ejecución

Puede haber momentos en que es preferible modificar las afinidades del CPU en huéspedes que estén ejecutándose, antes que reiniciarlos. Los comandos **virsh vcpuinfo** y **virsh vcpupin** pueden realizar modificaciones en las afinidades del CPU sobre huéspedes en ejecución.

El comando **virsh vcpuinfo** le ofrece información actualizada acerca de dónde se está ejecutando cada CPU virtual.

En nuestro ejemplo, *guest1* es un huésped con cuatro CPUs virtuales, siendo ejecutado en un equipo KVM.

```
# virsh vcpuinfo guest1
VCPU:           0
CPU:            3
State:          running
CPU time:       0.5s
CPU Affinity:   yyyyyyyy
VCPU:           1
CPU:            1
State:          running
CPU Affinity:   yyyyyyyy
VCPU:           2
CPU:            1
State:          running
CPU Affinity:   yyyyyyyy
VCPU:           3
CPU:            2
```

```
State:          running
CPU Affinity:   yyyyyyyy
```

La salida del comando **`virsh vcpuinfo`** (el valor **`yyyyyyyy`** de **`CPU Affinity`**), indica que el huésped puede en estos momentos ser ejecutado sobre cualquier CPU.

Para bloquear los CPUs virtuales para que utilicen el segundo nodo NUMA (CPUs cuatro a siete), ejecute los siguientes comandos.

```
# virsh vcpupin guest1 0 4
# virsh vcpupin guest1 1 5
# virsh vcpupin guest1 2 6
# virsh vcpupin guest1 3 7
```

El comando **`virsh vcpuinfo`** confirma el cambio en la afinidad.

```
# virsh vcpuinfo guest1
VCPU:           0
CPU:            4
State:          running
CPU time:       32.2s
CPU Affinity:   ----y---
VCPU:           1
CPU:            5
State:          running
CPU time:       16.9s
CPU Affinity:   -----y--
VCPU:           2
CPU:            6
State:          running
CPU time:       11.9s
CPU Affinity:   ------y-
VCPU:           3
CPU:            7
State:          running
CPU time:       14.6s
CPU Affinity:   -------y
```

Cierta información obtenida de los procesos KVM también puede confirmar que el huésped se está ejecutando sobre el segundo nodo NUMA.

```
# grep pid /var/run/libvirt/qemu/guest1.xml
<domstatus state='running' pid='4907'>
# grep Cpus_allowed_list /proc/4907/task/*/status
/proc/4907/task/4916/status:Cpus_allowed_list: 4
/proc/4907/task/4917/status:Cpus_allowed_list: 5
/proc/4907/task/4918/status:Cpus_allowed_list: 6
/proc/4907/task/4919/status:Cpus_allowed_list: 7
</section>
```

25.7. Cómo generar una nueva y única dirección MAC

En algunos casos, será necesario generar una nueva y única *dirección MAC* para un huésped. Hasta el momento de la redacción de esta guía, no existe aún una herramienta de línea de comandos disponible para hacerlo. El script que ofrecemos a continuación puede hacerlo. Guárdelo para que sea utilizado por su huésped como **`macgen.py`**. Ahora, desde ese directorio podrá ejecutar el script utilizando el comando **`./macgen.py`**, y una nueva dirección MAC será generada. Una salida de ejemplo debería parecerse a la siguiente:

```
$ ./macgen.py
00:16:3e:20:b0:11

#!/usr/bin/python
# macgen.py script to generate a MAC address for virtualized guests
#
import random
#
def randomMAC():
 mac = [ 0x00, 0x16, 0x3e,
  random.randint(0x00, 0x7f),
  random.randint(0x00, 0xff),
  random.randint(0x00, 0xff) ]
 return ':'.join(map(lambda x: "%02x" % x, mac))
#
print randomMAC()
```

Otro método para generar una nueva dirección MAC para su huésped

También puede utilizar los módulos de **python-virtinst** para generar una nueva dirección MAC, y **UUID** para utilizar en un archivo de configuración de huésped:

```
# echo  'import virtinst.util ; print\
 virtinst.util.uuidToString(virtinst.util.randomUUID())' | python
# echo  'import virtinst.util ; print virtinst.util.randomMAC()' | python
```

El script anterior puede también ser implementado como un archivo, de acuerdo a lo que se muestra más abajo.

```
#!/usr/bin/env python
#  -*- mode: python; -*-
print ""
print "New UUID:"
import virtinst.util ; print virtinst.util.uuidToString(virtinst.util.randomUUID())
print "New MAC:"
import virtinst.util ; print virtinst.util.randomMAC()
print ""
```

25.8. ftpd muy seguro

vsftpd puede ofrecer acceso hacia árboles de instalación desde un huésped para-virtualizado (por ejemplo, los repositorios de Fedora), o hacia otro tipo de datos. Si durante la instalación del servidor no ha instalado vsftpd, puede utilizar el paquete RPM desde el directorio **Server** de su medio de instalación, e instalarlo utilizando el comando **rpm -ivh vsftpd*.rpm** (tenga en cuenta que el paquete RPM debe estar en su directorio actual).

1. To configure vsftpd, edit **/etc/passwd** using **vipw** and change the ftp user's home directory to the directory where you are going to keep the installation trees for your para-virtualized guests. An example entry for the FTP user would look like the following:

   ```
   ftp:x:14:50:FTP User:/installtree/:/sbin/nologin
   ```

2. Verifique que vsftpd no esté habilitado utilizando el comando **chkconfig --list vsftpd**:

   ```
   $ chkconfig --list vsftpd
   ```

```
vsftpd          0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

3. Ejecute el comando **chkconfig --levels 345 vsftpd on** para iniciar automáticamente vsftpd en los niveles de ejecución 3, 4 y 5.

4. Utilice el comando **chkconfig --list vsftpd** para verificar que el demonio **vsftpd** esté habilitado para iniciarse junto con el arranque del sistema:

```
$ chkconfig --list vsftpd
vsftpd          0:off   1:off   2:off   3:on    4:on    5:on    6:off
```

5. Utilice el comando **service vsftpd start vsftpd** para iniciar el servicio vsftpd:

```
$service vsftpd start vsftpd
Starting vsftpd for vsftpd:                [  OK  ]
```

25.9. Cómo configurar persistencia LUN

La presente sección describe como implementar persistencia *LUN* sobre huéspedes y sobre el equipo anfitrión con y sin multipath.

Cómo implementar persistencia LUN sin multipath

Si su sistema no está utilizando multipath, puede utilizar **udev** para implementar una persistencia LUN. Antes de implementar persistencia LUN en su sistema, asegúrese que ha adquirido los UUIDs adecuados. Una vez que lo haya hecho, puede configurar persistencia LUN editando el archivo **scsi_id** dentro del directorio **/etc** . Una vez que haya abierto este archivo con un editor de textos, debe comentar la siguiente línea:

```
# options=-b
```

Luego reemplácela con el siguiente parámetro:

```
# options=-g
```

Esto le indica a udev que vigile a todos los dispositivos SCSI del sistema en busca de UUIDs. Para determinar los UUIDs del sistema, utilice el comando **scsi_id**:

```
# scsi_id -g -s /block/sdc
*3600a0b8000132751000015427b625e*
```

La cadena de caracteres más larga de la salida es el UUID. El UUID no se modifica cuando se agreguen nuevos dispositivos en el sistema. Obtenga el UUID de cada dispositivo para luego poder crear reglas para cada uno de ellos. Para crear nuevas reglas de dispositivos, edite el archivo **20-names.rules** del directorio **/etc/udev/rules.d** . La forma de denominar a las reglas de dispositivos tiene el siguiente formato:

```
# KERNEL="sd*",  BUS="scsi",  PROGRAM="sbin/scsi_id", RESULT="UUID", NAME="devicename"
```

Reemplace sus propios *UUID* y *devicename* con los obtenidos en la entrada del UUID de recién. La regla debería parecerse a la siguiente:

```
KERNEL="sd*",  BUS="scsi",  PROGRAM="sbin/scsi_id", RESULT="3600a0b80001327510000015427b625e",
 NAME="mydevicename"
```

Esto habilita a todos los dispositivos que se correspondan con el patrón **/dev/sd*** a ser inspeccionados en busca del UUID dado. Cuando encuentre un dispositivo coincidente, crea un dispositivo de nodo denominado */dev/devicename*. En nuestro ejemplo, el nodo de dispositivo es */dev/mydevice* . Por último, agregue la siguiente línea en el archivo **/etc/rc.local**:

```
/sbin/start_udev
```

Cómo implementar persistencia LUN con multipath

Para implementar una persistenacia LUN en un entorno multipath, primero debe definir los nombres apodos para los dispositivos multipath. En nuestro ejemplo, debe definir cuatro apodos para dispositivos editando el archivo **multipath.conf** dentro del directorio **/etc/**.

```
multipath  {
             wwid       3600a0b80001327510000015427b625e
             alias      oramp1
}
multipath  {
             wwid       3600a0b80001327510000015427b6
             alias      oramp2
}
multipath  {
             wwid       3600a0b80001327510000015427b625e
             alias      oramp3
}
multipath  {
             wwid       3600a0b80001327510000015427b625e
             alias      oramp4
}
```

Esto define 4 LUNs: **/dev/mpath/oramp1**, **/dev/mpath/oramp2**, **/dev/mpath/oramp3**, y **dev/mpath/oramp4**. Los dispositivos se ubicarán en el directorio **/dev/mpath** . Estos nombres LUN serán persistentes luego de reiniciarse, ya que se crean los apodos para los nombres en el wwid para cada uno de los LUNs.

25.10. Deshabilitar monitoreo de discos SMART para los huéspedes

El monitoreo de discos SMART puede deshabilitarse ya que estamos ejecutando sobre discos virtuales, y el almacenamiento físico es administrado por el equipo.

```
/sbin/service smartd stop
/sbin/chkconfig --del smartd
```

25.11. Cómo configurar un servidor VNC

To configure a VNC server use the **Remote Desktop** application in **System** > **Preferences**. Alternatively, you can run the **vino-preferences** command.

Las siguientes etapas configuran una sesión de servidor dedicado VNC:

1. Edite el archivo **~/.vnc/xstartup** para iniciar una sesión GNOME cada vez que **vncserver** sea iniciado. La primera vez que ejecute el script **vncserver**, se le preguntará si desea utilizar una contraseña con su sesión VNC.

2. Un ejemplo de archivo **xstartup**:

```
#!/bin/sh
# Uncomment the following two lines for normal desktop:
# unset SESSION_MANAGER
# exec /etc/X11/xinit/xinitrc
[ -x /etc/vnc/xstartup ] && exec /etc/vnc/xstartup
[ -r $HOME/.Xresources ] && xrdb $HOME/.Xresources
#xsetroot -solid grey
#vncconfig -iconic &
#xterm -geometry 80x24+10+10 -ls -title "$VNCDESKTOP Desktop" &
#twm &
if test -z "$DBUS_SESSION_BUS_ADDRESS" ; then
 eval `dbus-launch --sh-syntax –exit-with-session`
 echo "D-BUS per-session daemon address is: \
 $DBUS_SESSION_BUS_ADDRESS"
fi
exec  gnome-session
```

Parte V. Cuestiones relacionadas con el almacenamiento en virtualización

Introducción a la administración del almacenamiento para la virtualización

Esta sección describe la utilización de almacenamiento en red compartido en la virtualización en Fedora.

Los métodos siguientes funcionan en una virtualización:

- Canal de fibra
- iSCSI
- NFS
- GFS2

El almacenamiento de red es esencial para migraciones huéspedes, ya sean en línea o desconectados. No es posible migrar huéspedes sin disponer de un almacenamiento compartido.

Usando almacenamiento compartido con imágenes de disco virtuales

Este capitulo cubre el uso de varios tipos de dispositivos de almacenamiento compartido por la red para su uso como discos virtuales

26.1. Usando ISCSI para almacenar imágenes de discos virtuales.

Este capitulo cubre el uso de dispositivos basados en iSCSI para almacenar huéspedes virtuales.

26.2. Usando NFS para almacenar imágenes de discos virtuales

Este capitulo cubre el uso de NFS para almacenar huéspedes virtuales.

26.3. Usando GFS2 para almacenar discos virtuales.

Este capitulo trata acerca de la utilización de sistema de archivos global 2 de Red Hat (GFS2), para almacenar huéspedes virtuales

26.4. Grupos de almacenamiento

Utilizando grupos de almacenamiento en RHEL

26.4.1. Configurando dispositivos de almacenamiento para grupos

Como configurar el dispositivo/RHEL para grupos de almacenamiento como iSCSI, GFS y a lo mejor Canales de Fibra.

26.4.2. Direccionamiento virtualizado de los huéspedes a los grupos de almacenamiento

Ejemplo de direccionamiento de los grupos de almacenamiento libvirt

Parte VI. Guía de referencia de virtualización

Los comandos de virtualización, herramients del sistema, aplicaciones y referencia de sistemas adicionales

Estos capítulos proporcionan descripciones detalladas sobre los comandos de virtualización, las herramientas del sistema y las aplicaciones incluidas en Fedora. Estos capítulos están diseñados para usuarios que requieren información en la funcionalidad avanzada y otras características.

Herramientas de virtualización

A continuación ofrecemos una lista con herramientas para administración de virtualizaciones, para realizar depuraciones y para trabajar en entornos de red.

Herramientas de administración de sistemas

- **vmstat**
- **iostat**
- **lsof**
- **qemu-img**

Herramientas avanzadas de depuración

- **systemTap**
- **crash**
- **sysrq**
- **sysrq t**
- **sysrq w**
- **sysrq c**

Creación de redes

brtcl

- ```
  # brctl show
  bridge name bridge id  STP enabled interfaces
  pan0  8000.000000000000 no
  virbr0  8000.000000000000 yes
  ```
- ```
  # brctl showmacs virbr0
  port no mac addr  is local? ageing timer
  ```
- ```
  # brctl showstp virbr0
  virbr0
   bridge id  8000.000000000000
   designated root 8000.000000000000
   root port     0   path cost     0
   max age    19.99   bridge max age    19.99
   hello time     1.99   bridge hello time    1.99
   forward delay     0.00   bridge forward delay    0.00
   ageing time   299.95
   hello timer     1.39   tcn timer     0.00
   topology change timer    0.00   gc timer     0.39
  ```

- **ifconfig**
- **tcpdump**
  ```

Herramientas KVM

- **ps**
- **pstree**
- **top**
- **kvmtrace**
- **kvm_stat**

Administración de huéspedes virtuales con virsh

virsh es una herramienta de línea de comando para administrar a los huéspedes y al hipervisor.

La herramienta **virsh** se crea en la API de administración **libvirt** y funciona como una alternativa para el comando **xm** y el Administrador de huésped gráfico (**virt-manager**). **virsh** puede ser utilizado en modo de sólo lectura por usuarios sin privilegios. Se puede utilizar **virsh** para ejecutar scripts para las máquinas de huésped.

referencia rápida del comando virsh

La siguientes tablas son una rápida referencia para todas las opciones de línea de comandos de virsh.

Comando	Descripción
help	Imprime información de ayuda básica.
list	Lista todos los huéspedes.
dumpxml	Entrega el archivo de configuración XML para el huésped.
create	Crea un huésped desde un archivo de configuración XML e inicia el nuevo huésped.
start	Inicia un huésped inactivo.
destroy	Obliga a un huésped a detenerse.
define	Entrega un archivo de configuración XML para un huésped.
domid	Displays the guest's ID.
domuuid	Displays the guest's UUID.
dominfo	Muestra información de huésped.
domname	Displays the guest's name.
domstate	Muestra el estado de un huésped.
quit	Sale de la terminal interactiva.
reboot	Reinicia un huésped.
restore	Restaura una sesión guardada anteriormente en un archivo.
resume	Reanuda un huésped en pausa.
save	Guarda el estado de un huésped en un archivo
shutdown	Apaga un huésped de forma apropiada.
suspend	Pone en pausa a un huésped.
undefine	Borra todos los archivos asociados con un huésped.
migrate	Migra un huésped a otros host.

Tabla 28.1. Comandos de administración de huésped

Las siguientes opciones del comando **virsh** se utilizan para administrar recursos del huésped, y del hipervisor:

Comando	Descripción
setmem	Establece la memoria asignada para un huésped.
setmaxmem	Establece el límite máximo de memoria para el hipervisor.
setvcpus	cambia el número de CPU virtuales asignadas a un huésped.
vcpuinfo	Muestra información de CPU virtual sobre un huésped.
vcpupin	Controla la afinidad de CPU virtual de un huésped.
domblkstat	Muestra las estadísticas de dispositivo de bloque para un huésped en ejecución.
domifstat	Muestra estadísticas de interfaz de red para un huésped en ejecución.
attach-device	Conecta un dispositivo a un huésped, mediante la definición de un dispositivo en un archivo XML.
attach-disk	Conecta un nuevo dispositivo de disco para un huésped.
attach-interface	Conecta una nueva interfaz de red para un huésped.
detach-device	Desconecta un dispositivo de un huésped, adquiere la misma clase de descripciones del comando **attach-device**.
detach-disk	Desconecta un dispositivo de disco desde un huésped.
detach-interface	Desconecta una interfaz de red de un huésped.

Tabla 28.2. Opciones de administración de recursos

Estas son las opciones misceláneas de **virsh**:

Comando	Descripción
version	Muestra la versión de **virsh**
nodeinfo	Entrega información acerca del hipervisor

Tabla 28.3. Opciones misceláneas

Conexión al hipervisor

Conectar a la sesión del hipervisor con **virsh**:

```
# virsh connect {hostname OR URL}
```

Where **<name>** is the machine name of the hypervisor. To initiate a read-only connection, append the above command with **-readonly**.

Creación de un volcado de máquina virtual XML (archivo de configuración)

Output a guest's XML configuration file with **virsh**:

```
# virsh dumpxml {guest-id, guestname or uuid}
```

This command outputs the guest's XML configuration file to standard out (**stdout**). You can save the data by piping the output to a file. An example of piping the output to a file called *guest.xml*:

```
# virsh dumpxml GuestID > guest.xml
```

Este archivo **guest.xml** puede volver a crear el huésped (consulte *Editing a guest's configuration file*). Puede editar este archivo de configuración XML para configurar dispositivos adicionales o para utilizar huéspedes adicionales. Para obtener mayor información acerca de la modificación de archivos creados con **virsh dumpxml**, consulte la *Sección 31.1, “Uso de los archivos de configuración XML con virsh”*.

Un ejemplo de salida de **virsh dumpxml**:

```
# virsh dumpxml r5b2-mySQL01
<domain type='kvm' id='13'>
    <name>r5b2-mySQL01</name>
    <uuid>4a4c59a7ee3fc78196e4288f2862f011</uuid>
    <bootloader>/usr/bin/pygrub</bootloader>
    <os>
        <type>linux</type>
        <kernel>/var/lib/libvirt/vmlinuz.2dgnU_</kernel>
 <initrd>/var/lib/libvirt/initrd.UQafMw</initrd>
        <cmdline>ro root=/dev/VolGroup00/LogVol00 rhgb quiet</cmdline>
    </os>
    <memory>512000</memory>
    <vcpu>1</vcpu>
    <on_poweroff>destroy</on_poweroff>
    <on_reboot>restart</on_reboot>
    <on_crash>restart</on_crash>
    <devices>
        <interface type='bridge'>
            <source bridge='br0'/>
            <mac address='00:16:3e:49:1d:11'/>
            <script path='bridge'/>
        </interface>
        <graphics type='vnc' port='5900'/>
        <console tty='/dev/pts/4'/>
    </devices>
</domain>
```

Creación de un huésped desde el archivo de configuración

Los huéspedes pueden ser creados desde los archivos de configuración XML. Se pueden copiar los XML existentes de los huéspedes creados anteriormente, o utilizar la opción **dumpxml** (consulte *Creación de un volcado de máquina virtual XML (archivo de configuración)*). Para crear un huésped desde un archivo XML con **virsh**:

```
# virsh create configuration_file.xml
```

Editing a guest's configuration file

En lugar de utilizar la opción **dumpxml** (consulte *Creación de un volcado de máquina virtual XML (archivo de configuración)*), los huéspedes pueden ser editados o bien cuando estén en ejecución, o bien cuando estén desconectados. El comando **virsh edit** proporciona esta funcionalidad. Por ejemplo, para editar el huésped llamado *softwaretesting*:

```
# virsh edit softwaretesting
```

Éste abre un editor de texto. El editor de texto predeterminado es el parámetro de shell **$EDITOR** (configure **vi** por defecto).

Suspender un huésped

Suspende un huésped con **virsh**:

```
# virsh suspend {domain-id, domain-name or domain-uuid}
```

Cuando un huésped se encuentra en estado suspendido, consume memoria RAM del sistema, pero no recursos de procesador. Mientras el huésped continúe en este estado, no estarán disponibles ni los discos, ni la entrada o la salida de red. Esta operación es inmediata y el huésped puede ser reiniciado con la opción **resume** (*Reanudar un huésped*).

Reanudar un huésped

Restaure un huésped suspendido con **virsh** mediante la opción **resume**:

```
# virsh resume {domain-id, domain-name or domain-uuid}
```

Esta operación es inmediata y los parámetros de huésped son preservados para operaciones **suspend** y **resume**.

Guardar un huésped

Guarde el estado actual de un huésped en un archivo mediante el comando **virsh**:

```
# virsh save {domain-name, domain-id or domain-uuid} filename
```

Este comando detiene el huésped determinado y guarda los datos en un archivo, lo cual puede demorar algún tiempo dependiendo de la cantidad de memoria que el huésped esté utilizando. Puede restablecer el estado del huésped con la opción **restore** (*Restaurar un huésped*). 'Guardar' funciona en forma similar a realizar una pausa: en vez de simplemente poner en pausa a un huésped, el estado actual del huésped es guardado.

Restaurar un huésped

Restaura un huésped guardado previamente con el comando **virsh save** (*Guardar un huésped*), mediante **virsh**:

```
# virsh restore filename
```

This restarts the saved guest, which may take some time. The guest's name and UUID are preserved but are allocated for a new id.

Apagar un huésped

Apaga un huésped mediante el comando **virsh**:

```
# virsh shutdown {domain-id, domain-name or domain-uuid}
```

You can control the behavior of the rebooting guest by modifying the **on_shutdown** parameter in the guest's configuration file.

Reiniciar un huésped

Reiniciar un huésped mediante el comando **virsh**:

```
#virsh reboot {domain-id, domain-name or domain-uuid}
```

You can control the behavior of the rebooting guest by modifying the **on_reboot** element in the guest's configuration file.

Forzar al huésped a detenerse

Obliga a un huésped a detenerse con el comando **virsh**:

```
# virsh destroy {domain-id, domain-name or domain-uuid}
```

Este comando apaga y detiene en forma abrupta el huésped determinado. Si utiliza **virsh destroy**, pueden llegar a corromperse los sistemas de archivo del huésped. Utilice la opción **destroy** sólo si el huésped no responde. Para huéspedes para-virtualizados, utilice en su lugar la opción **shutdown** (*Apagar un huésped*).

Obtener el ID de dominio de un huésped

Para obtener el ID de dominio de un huésped:

```
# virsh domid {domain-name or domain-uuid}
```

Obtener el nombre de dominio de un huésped

Para obtener el nombre de dominio de un huésped:

```
# virsh domname {domain-id or domain-uuid}
```

Obtener el UUID para un huésped

Para obtener el Identificador único universal (UUID) para un huésped:

```
# virsh domuuid {domain-id or domain-name}
```

Un ejemplo de la salida de **virsh domuuid**:

```
# virsh domuuid r5b2-mySQL01
4a4c59a7-ee3f-c781-96e4-288f2862f011
```

Mostrar la información de huésped

Using **virsh** with the guest's domain ID, domain name or UUID you can display information on the specified guest:

```
# virsh dominfo {domain-id, domain-name or domain-uuid}
```

Este es un ejemplo de salida de **virsh dominfo**:

```
# virsh dominfo r5b2-mySQL01
id:             13
name:           r5b2-mysql01
uuid:           4a4c59a7-ee3f-c781-96e4-288f2862f011
os type:       linux
state:          blocked
cpu(s):         1
cpu time:      11.0s
max memory:     512000 kb
used memory:    512000 kb
```

Mostrar información del host

Para ver información sobre el huésped:

```
# virsh nodeinfo
```

Un ejemplo de salida de **virsh nodeinfo**:

```
# virsh nodeinfo
CPU model                    x86_64
CPU (s)                      8
CPU frequency                2895 Mhz
CPU socket(s)                2
Core(s) per socket           2
Threads per core:            2
Numa cell(s)                 1
Memory size:                 1046528 kb
```

Se muestra la información del nodo y de la máquina que soporta el proceso de virtualización.

Mostrar los huéspedes

Para ver la lista de huéspedes y su estado actual con **virsh**:

```
# virsh list
```

Otras opciones incluyen:

La opción **--inactive** para listar los huéspedes inactivos (es decir, los huéspedes que han sido definidos pero que no están activos) y

La opción **--all** lista todos los huéspedes. Por ejemplo:

```
# virsh list --all
 Id Name                 State
----------------------------------
```

```
 0 Domain-0             running
 1 Domain202            paused
 2 Domain010            inactive
 3 Domain9600           crashed
```

La salida desde **`virsh list`** se categoriza como uno de los seis estados (listados abajo).

- El estado **`running`** se refiere a los huéspedes que están actualmente activos en una CPU.
- Los huéspedes listados como **`blocked`** están bloqueados y no se están ejecutando o no son ejecutables. Esto es causado por un huésped esperando en E/S (un estado de espera tradicional) o huéspedes en modo durmiente.
- El estado **`paused`** lista los dominios que están en pausa. Esto se presenta si un administrador utiliza el botón **`pause`** en **`virt-manager`**, **`xm pause`** o **`virsh suspend`**. Cuando un huésped es puesto en pausa, consume memoria y otros recursos, pero no tiene derecho a programación ni recursos de CPU desde el hipervisor.
- El estado **`shutdown`** es para huéspedes en el proceso de apagado. El huésped recibe una señal de apagado y debe estar en el proceso de detener las operaciones correctamente. Esto puede que no funcione para todos los sistemas operativos, algunos sistemas operativos no responden a estas señales.
- Los dominios en el estado **`dying`** están en el proceso de muerte, el cual es el estado en el que el dominio no se ha bloqueado o apagado totalmente.
- Los huéspedes de **`crashed`** han fallado en la ejecución y ya no funcionan. Este estado sólo puede ocurrir si el huésped ha sido configurado para no reiniciarse en bloqueo.

Mostrar información de la CPU virtual

Para ver la información de la CPU virtual desde un huésped con **`virsh`**:

```
# virsh vcpuinfo {domain-id, domain-name or domain-uuid}
```

Un ejemplo de salida de **`virsh vcpuinfo`**:

```
# virsh vcpuinfo r5b2-mySQL01
VCPU:           0
CPU:            0
State:          blocked
CPU time:       0.0s
CPU Affinity:   yy
```

Configurar la afinidad de la CPU virtual

Para configurar la afinidad de la CPU virtual con las CPU físicas:

```
# virsh vcpupin domain-id vcpu cpulist
```

The **`domain-id`** parameter is the guest's ID number or name.

El parámetro **`vcpu`** indica la cantidad de CPUs virtualizadas alojadas en el huésped. El parámetro **`vcpu`** debe ser ofrecido.

El parámetro **cpulist** es una lista de números identificadores de CPU separada por comas. El parámetro **cpulist** determina sobre qué CPUs físicos pueden ejecurtarse los VCPUs.

Configurar la cuenta de CPU virtual

Para modificar el número de CPU asignadas a un huésped con **virsh**:

```
# virsh setvcpus {domain-name, domain-id or domain-uuid} count
```

El nuevo valor *count* no puede exceder la cuenta de la cantidad que se especificó durante la creación del huésped.

Configurar la asignación de memoria

To modify a guest's memory allocation with **virsh** :

```
# virsh setmem {domain-id or domain-name} count
```

Debe especificar la *cuenta* en kilobytes. La nueva cantidad no puede exceder la cantidad especificada durante la creación del huésped. Los valores inferiores a 64 MB probablemente no funcionarán con la mayor parte de sistemas operativos de huésped. La cantidad máxima de memoria no afectará al huésped activo: Si el nuevo valor es menor, la memoria disponible disminuirá, y el huésped podría caerse.

Mostrar información de dispositivo de bloque de huésped

Utilice **virsh domblkstat** para ver las estadísticas del dispositivo de bloque para un huésped en ejecución.

```
# virsh domblkstat GuestName block-device
```

Mostrar información del dispositivo de red de huésped

Use **virsh domifstat** para ver las estadísticas de interfaz de red para un huésped en ejecución.

```
# virsh domifstat GuestName interface-device
```

Migrar huéspedes con virsh

Un huésped puede ser migrado a otro host con **virsh**. Para migrar el dominio a otro host, añada --live para migración en vivo. El comando **migrate** acepta parámetros en el siguiente formato:

```
# virsh migrate --live GuestName DestinationURL
```

El parámetro *--live* es opcional. Añada el parámetro *--live* para migraciones en vivo.

El parámetro *GuestName* representa es el nombre huésped que desea migrar.

El parámetro *DestinationURL* es la URL o el nombre del equipo del sistema de destibo. El sistema de destino necesita:

- Fedora 9, o más recientes,

- la misma versión del hipervisor, y
- el servicio **`libvirt`** debe ser iniciado.

Una vez que el comando haya sido ingresado, le será solicitada la contraseña de usuario root del sistema de destino.

Administrar redes virtuales

Esta sección cubre el manejo de redes virtuales con el comando **`virsh`**. Para listar las redes virtuales:

```
# virsh net-list
```

Este comando genera un mensaje de salida similar al siguiente:

```
# virsh net-list
Name                 State      Autostart
-----------------------------------------
default              active     yes
vnet1              active     yes
vnet2              active     yes
```

Para ver la información de red específica de una red virtual utilice:

```
# virsh net-dumpxml NetworkName
```

Este comando muestra la información sobre la red virtual especificada en formato XML:

```
# virsh net-dumpxml vnet1
<network>
  <name>vnet1</name>
  <uuid>98361b46-1581-acb7-1643-85a412626e70</uuid>
  <forward dev='eth0'/>
  <bridge name='vnet0' stp='on' forwardDelay='0' />
  <ip address='192.168.100.1' netmask='255.255.255.0'>
    <dhcp>
      <range start='192.168.100.128' end='192.168.100.254' />
    </dhcp>
  </ip>
</network>
```

Otros comandos de **`virsh`** para administrar redes virtuales son:

- **`virsh net-autostart`** ***`nombre-de_red`*** — Autoinicia una red especificada como *`nombre_de_ red`*.
- **`virsh net-create`** ***`XMLfile`*** — genera e inicia una nueva red mediante un archivo XML existente.
- **`virsh net-define`** ***`XMLfile`*** — genera un nuevo dispositivo de red desde un archivo XML existente sin iniciarlo.
- **`virsh net-destroy`** ***`[nombre de red]`*** — destruye la red especificada en [nombre de red]
- **`virsh net-name`** ***`networkUUID`*** — convierte un *`UUID_de_red`* determinado para un nombre de red.

- **virsh net-uuid *nombre_de _red*** — convierte un *nombre_ de_ red* determinado para un UUID de red.
- **virsh net-start *nombre_de_red_inactiva*** — inicia una red inactiva.
- **virsh net-undefine *nombre_de_una_red_inactiva*** — elimina la definición de una red inactiva.

Manejo de huéspedes con un Administrador de máquinas virtuales (virt-manager)

Esta sección describe las ventanas del Administrador de máquinas virtuales (**`virt-manager`**), cuadros de diálogos y varios controles GUI.

El **`virt-manager`** proporciona una vista gráfica de hipervores y huéspedes en su sistema y máquinas remotas. El **`virt-manager`** sirve para definir tanto los huéspedes para-virtualizados como los completamente virtualizados. El **`virt-manager`** puede realizar tareas de administración de virtualización, incluyendo:

- asignación de memoria,
- asignación de CPU virtuales,
- monitorización de rendimiento operacional,
- ahorro y restauración, pausa y reanudación y apagado e inicialización de huéspedes virtualizados,
- enlaces a consolas de gráficas y textuales, y
- Migraciones en vivo y desconectadas.

29.1. La ventana de agregado de conexión

Esta ventana aparece primero y le pide al usuario escoger una sesión de hipervisor. Los usuarios sin privilegios pueden iniciar una sesión de sólo escritura. Los usuarios root pueden iniciar una sesión con estado completo de lectura y escritura. Para un uso normal, seleccione la opción QEMU para KVM.

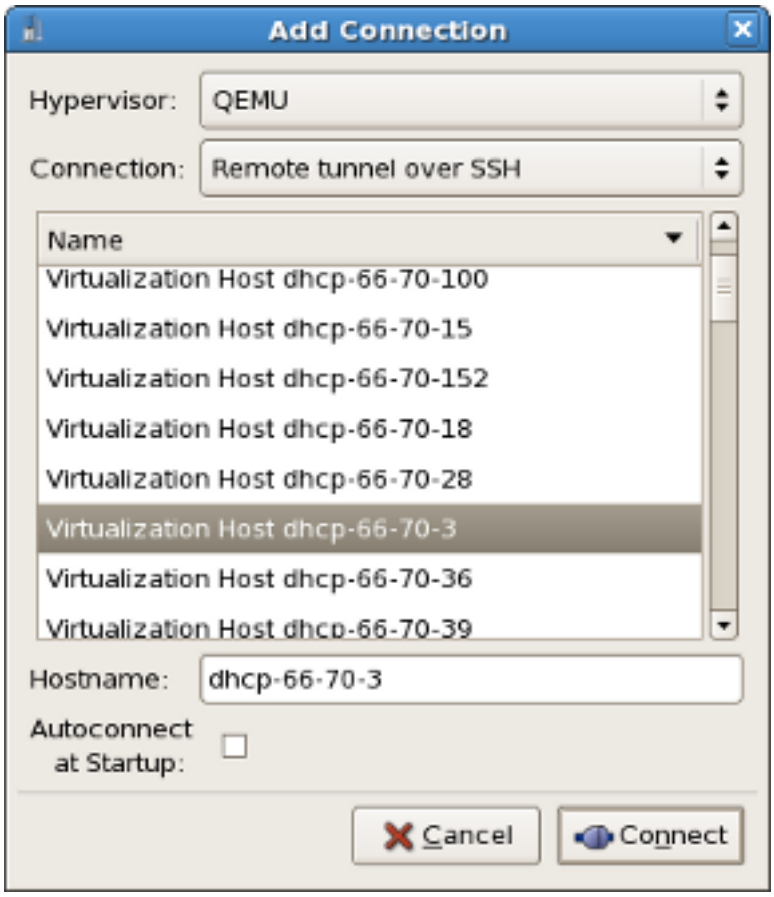


Figura 29.1. Ventana de conexión del Administrador de máquinas virtuales

29.2. La ventana principal del Administrador de máquinas virtuales

This main window displays all the running guests and resources used by guests. Select a virtualized guest by double clicking the guest's name.

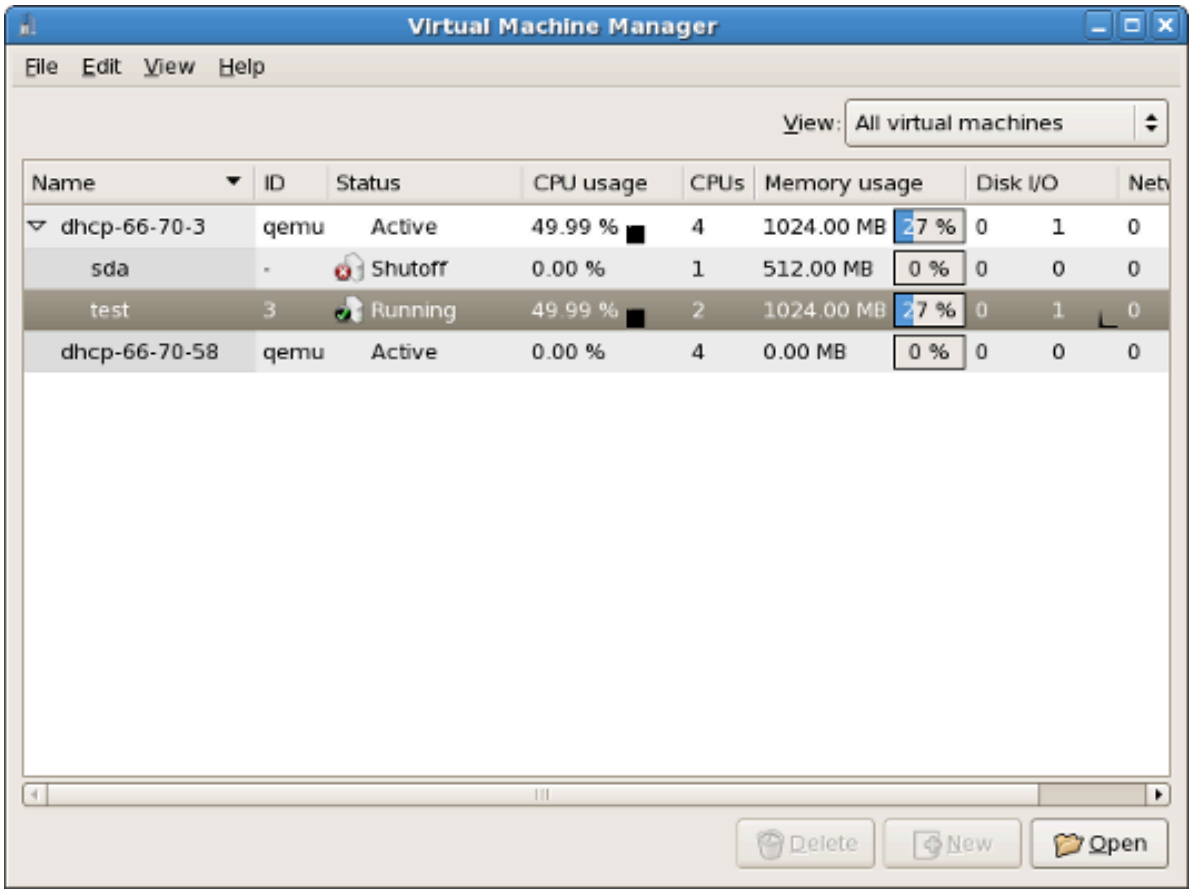

Virtual Machine Manager
File Edit View Help
View: All virtual machines
Name ID Status CPU usage CPUs Memory usage Disk I/O Net
dhcp-66-70-3 qemu Active 49.99 % 4 1024.00 MB 27 % 0 1 0
sda - Shutoff 0.00 % 1 512.00 MB 0 % 0 0 0
test 3 Running 49.99 % 2 1024.00 MB 27 % 0 1 0
dhcp-66-70-58 qemu Active 0.00 % 4 0.00 MB 0 % 0 0 0
Delete New Open

Figura 29.2. Ventana principal del Administrador de máquinas virtuales

29.3. La pestaña de visión general del huésped

The **Overview** tab displays graphs and statistics of a guest's live resource utilization data available from **`virt-manager`**. The UUID field displays the globally unique identifier for the virtual machines.

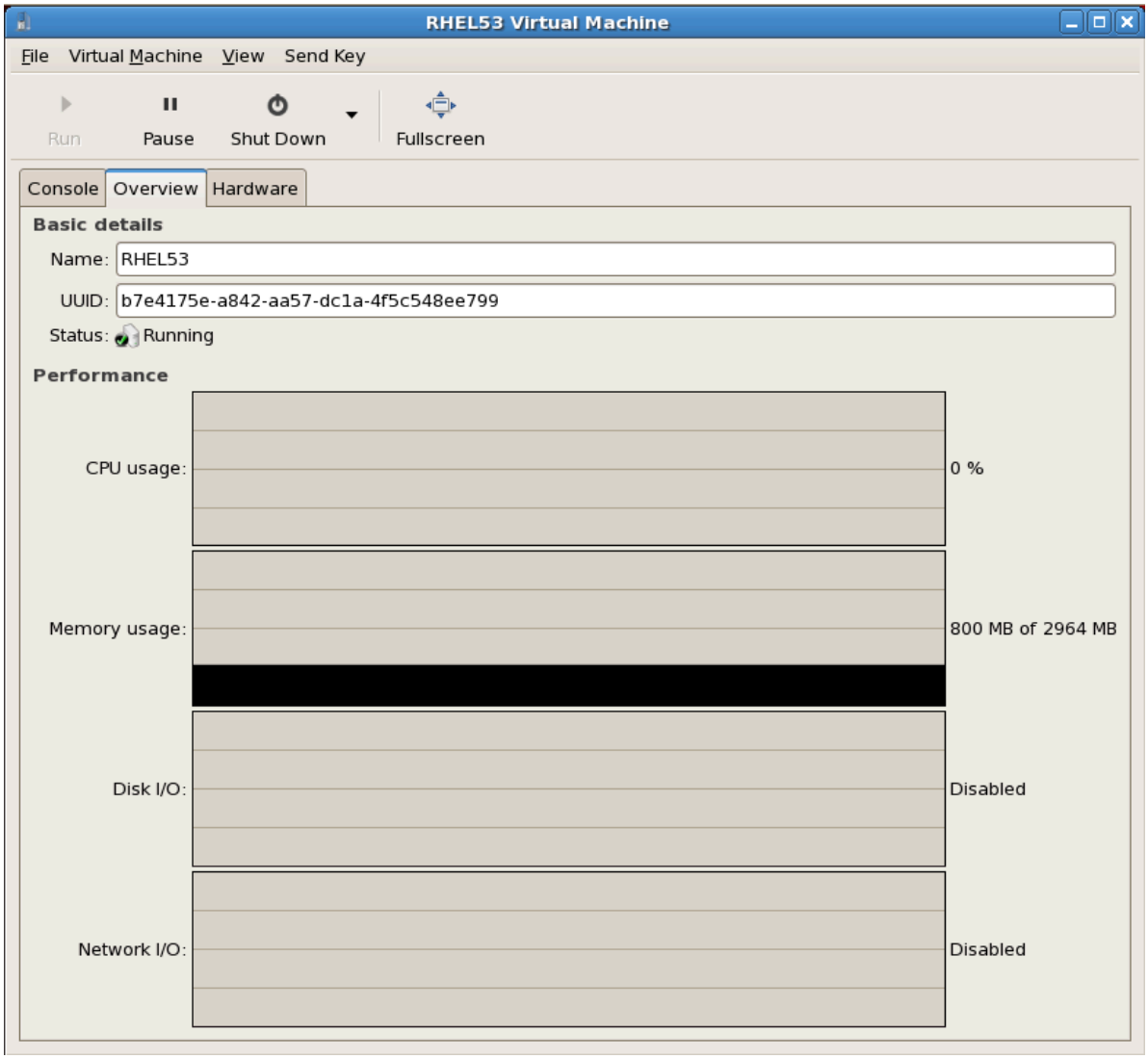


Figura 29.3. La pestaña de **Resumen**

29.4. Consola gráfica de la Máquina virtual

This window displays a virtual machine's graphical console. Para-virtualized and fully virtualized guests use different techniques to export their local virtual framebuffers, but both technologies use **VNC** to make them available to the Virtual Machine Manager's console window. If your virtual machine is set to require authentication, the Virtual Machine Graphical console prompts you for a password before the display appears.

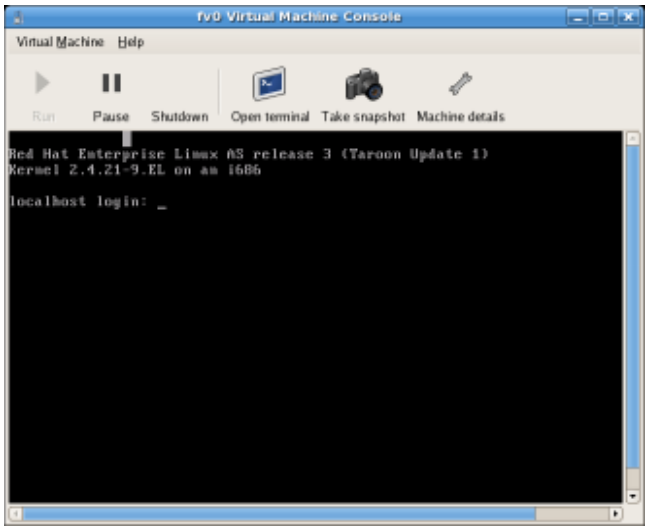


Figura 29.4. Ventana de la consola gráfica

Una observación sobre seguridad y VNC

VNC is considered insecure by many security experts, however, several changes have been made to enable the secure usage of VNC for virtualization. The guest machines only listen to the local host (`dom0`)'s loopback address (`127.0.0.1`). This ensures only those with shell privileges on the host can access virt-manager and the virtual machine through VNC.

La administración remota puede realizarse siguiendo las instrucciones en el *Capítulo 21, Administración remota de huéspedes virtualizados*. TLS puede proporcionar seguridad de nivel empresarial para administrar sistemas invitados y anfitriones.

Your local desktop can intercept key combinations (for example, Ctrl+Alt+F11) to prevent them from being sent to the guest machine. You can use **`virt-manager`**sticky key' capability to send these sequences. You must press any modifier key (Ctrl or Alt) 3 times and the key you specify gets treated as active until the next non-modifier key is pressed. Then you can send Ctrl-Alt-F11 to the guest by entering the key sequence 'Ctrl Ctrl Ctrl Alt+F1'.

Pruebe el protocolo abierto SPICE (Simple Protocol for Independent Computing Environment).

29.5. Cómo iniciar virt-manager

Para iniciar una sesión del **`virt-manager`** abra el menú de **Aplicaciones**; luego **Herramientas del sistema** y seleccione **Administrador de máquina virtual** (**`virt-manager`**).

La ventana principal de **`virt-manager`** aparece.

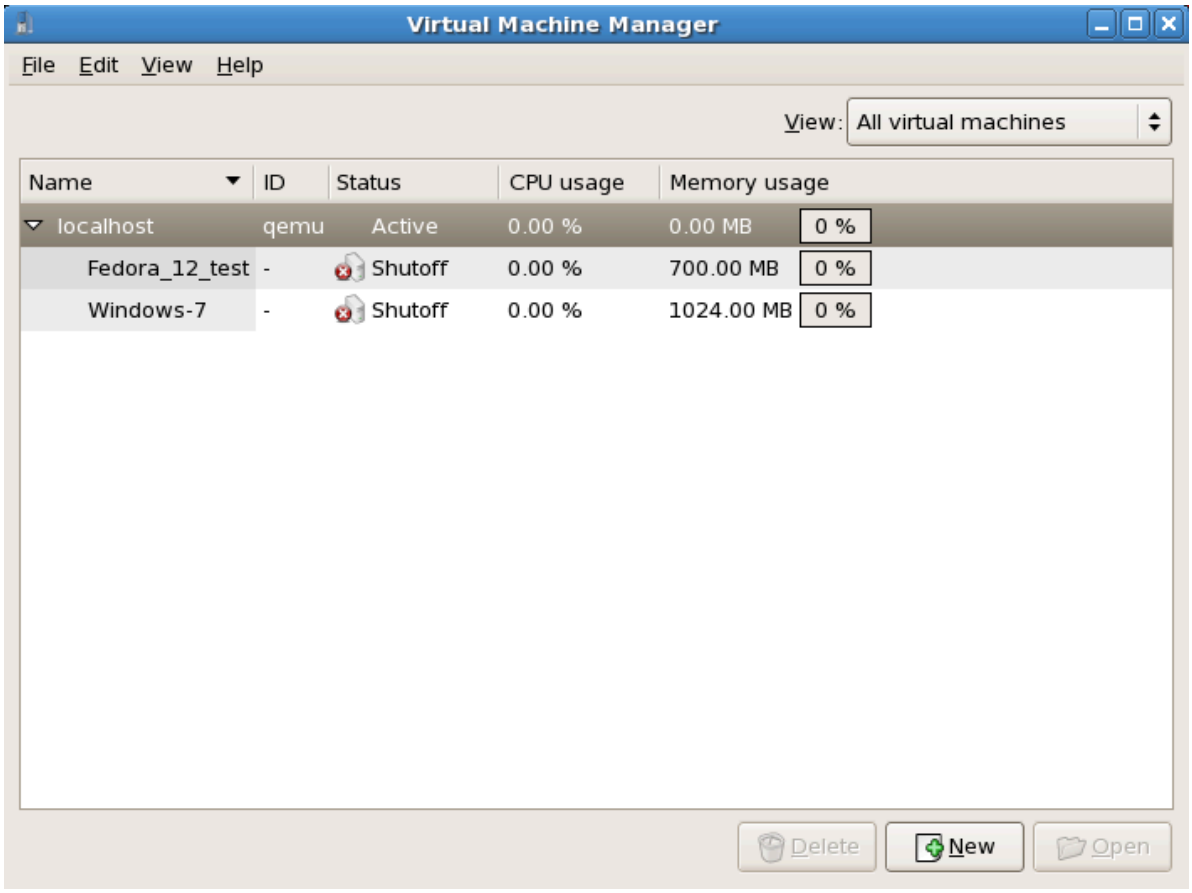

Virtual Machine Manager
File Edit View Help
View: All virtual machines
Name ID Status CPU usage Memory usage
localhost qemu Active 0.00 % 0.00 MB 0 %
Fedora_12_test - Shutoff 0.00 % 700.00 MB 0 %
Windows-7 - Shutoff 0.00 % 1024.00 MB 0 %
Delete New Open

Figura 29.5. Inicio de **virt-manager**

Alternativamente, **virt-manager** puede iniciarse remotamente utilizando ssh como se demuestra con el siguiente comando:

```
ssh -X host's address[remotehost]# virt-manager
```

La utilización de **ssh** para manejar equipos y máquinas virtuales se explica más adelante en la *Sección 21.1, "Administración remota con SSH"*.

29.6. Restaurar una máquina guardada

Una vez iniciado el administrador de máquinas virtuales, todas las máquinas en su sistema aparecerán en la ventana principal. Domain0 es su sistema anfitrión. Si no hay máquinas ejecutándose en el sistema, nada aparecerá en la ventana.

Para restaurar una sesión guardada anteriormente

1. Desde el menú **Archivo**, seleccione **Restaurar máquina guardada**.

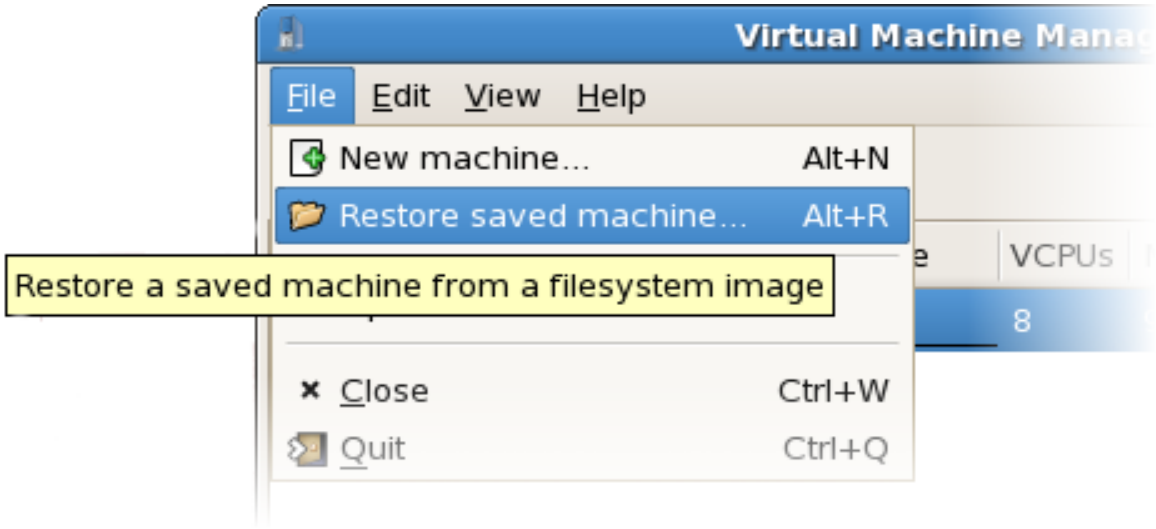


Figura 29.6. Restauración de una máquina virtual

2. La ventana principal de **Restaurar máquina virtual** aparece.
3. Vaya al directorio correcto y seleccione el archivo de sesión guardado.
4. Haga clic en **Abrir**.

El sistema virtual guardado aparecerá en la ventana principal del administrador de máquinas virtuales.

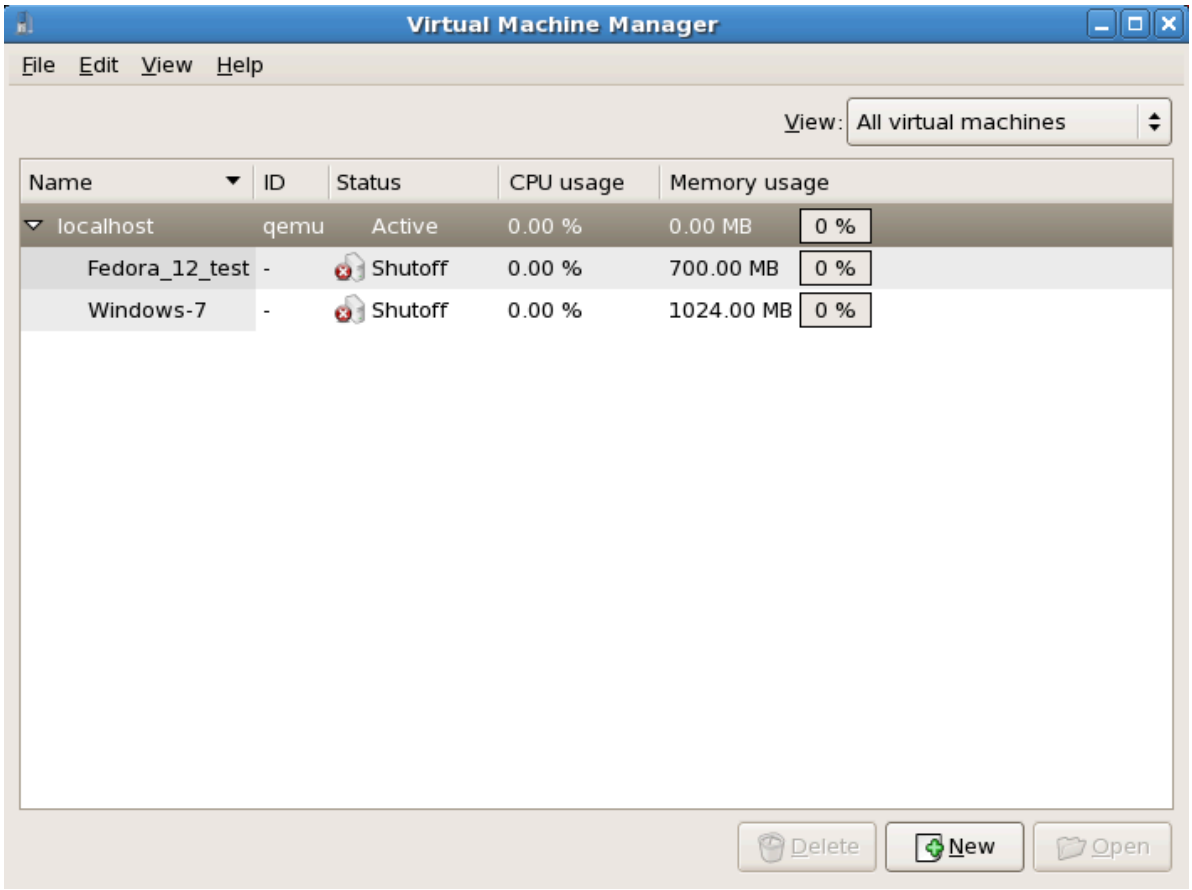

Virtual Machine Manager
File Edit View Help
View: All virtual machines
Name ID Status CPU usage Memory usage
localhost qemu Active 0.00 % 0.00 MB 0 %
Fedora_12_test - Shutoff 0.00 % 700.00 MB 0 %
Windows-7 - Shutoff 0.00 % 1024.00 MB 0 %
Delete New Open

Figura 29.7. La sesión restaurada del administrador de máquinas virtuales

29.7. Mostrar información de huéspedes

Puede ver el monitor de máquinas virtuales para ver información de la actividad de cualquier máquina virtual en su sistema.

To view a virtual system's details:

1. En la ventana principal del administrador de máquinas virtuales, resalte la máquina virtual que desea ver.

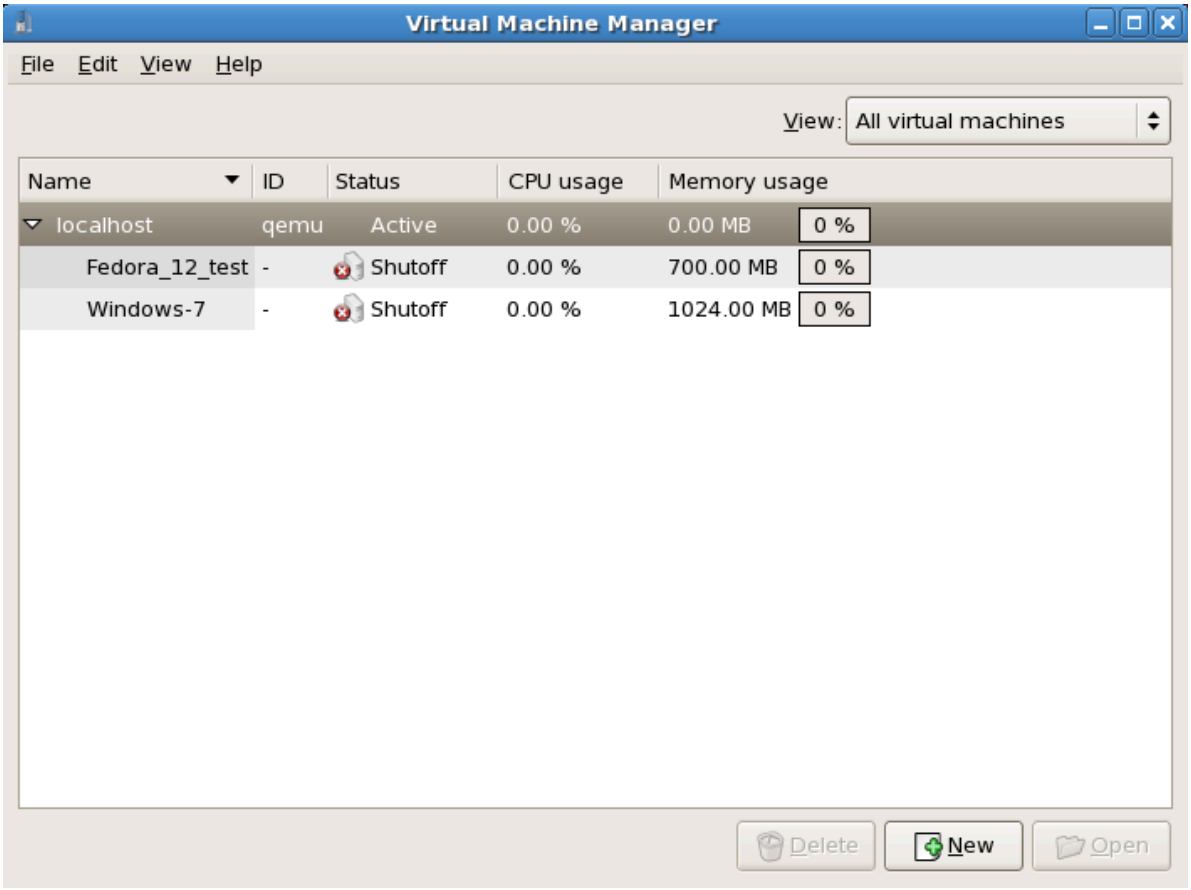

Virtual Machine Manager
File Edit View Help
View: All virtual machines
Name ID Status CPU usage Memory usage
localhost qemu Active 0.00 % 0.00 MB 0 %
Fedora_12_test - Shutoff 0.00 % 700.00 MB 0 %
Windows-7 - Shutoff 0.00 % 1024.00 MB 0 %
Delete New Open

Figura 29.8. Para seleccionar la máquina virtual

2. Desde el menú **Editar** del administrador de máquinas virtuales seleccione **Detalles de la máquina** (o haga clic en el botón **Detalles** en la parte inferior de la ventana principal del administrador de máquinas virtuales).

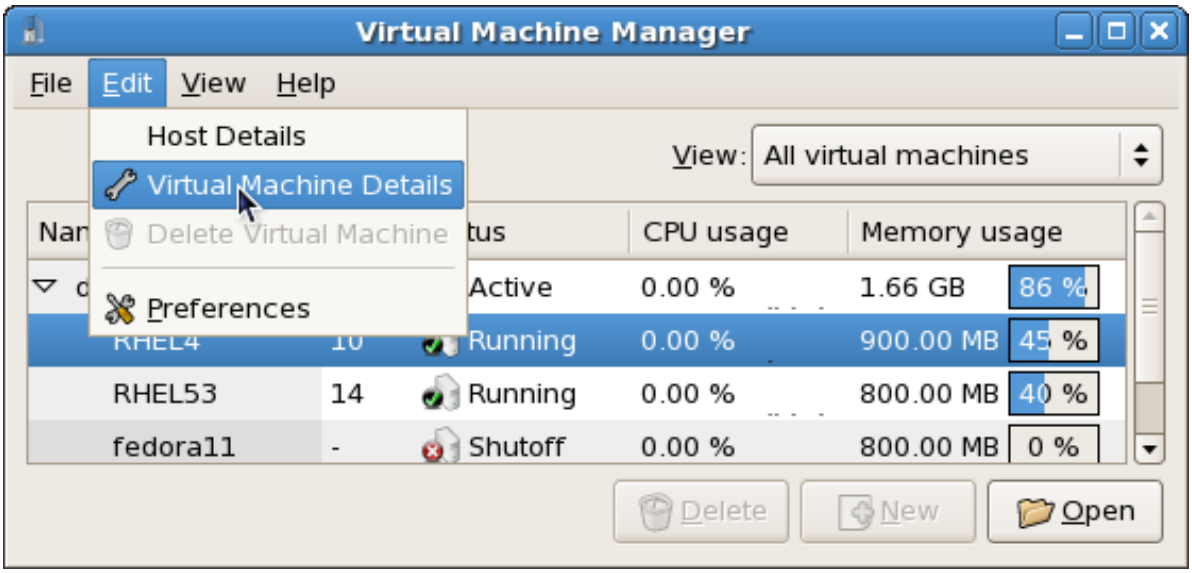


Figura 29.9. Mostrar la ventana de información general

En la ventana de **Máquina virtual**, haga clic en la pestaña de **Resumen**.

La pestaña **Overview** reune la información relacionada con la utilización de la memoria y del CPU que esté realizando el huésped virtualizado especificado.

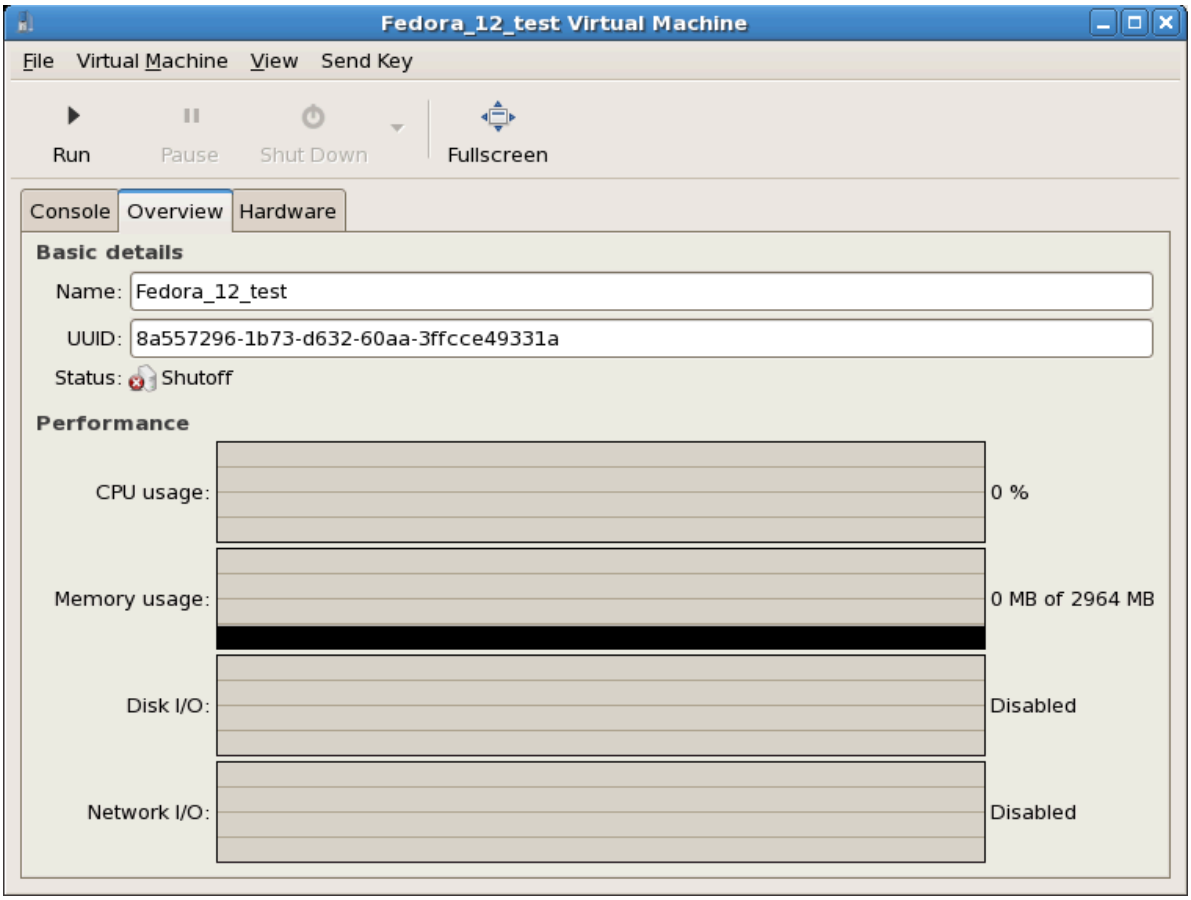


Figura 29.10. Mostrar información general de huésped

3. En la ventana de **Máquina virtual**, haga clic en la pestaña de **Hardware**.

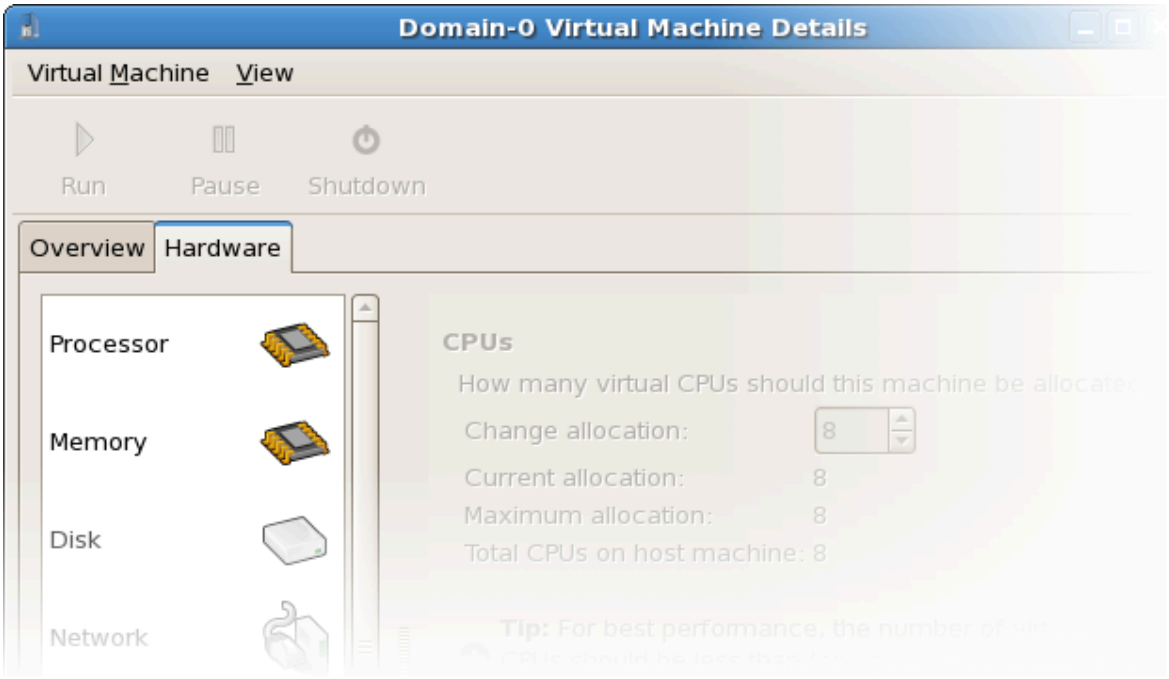


Figura 29.11. Muestra de detalles de hardware del huésped

4. En la pestaña **Hardware**, haga clic en **Procesador** para ver o cambiar la asignación de memoria del procesador actual.

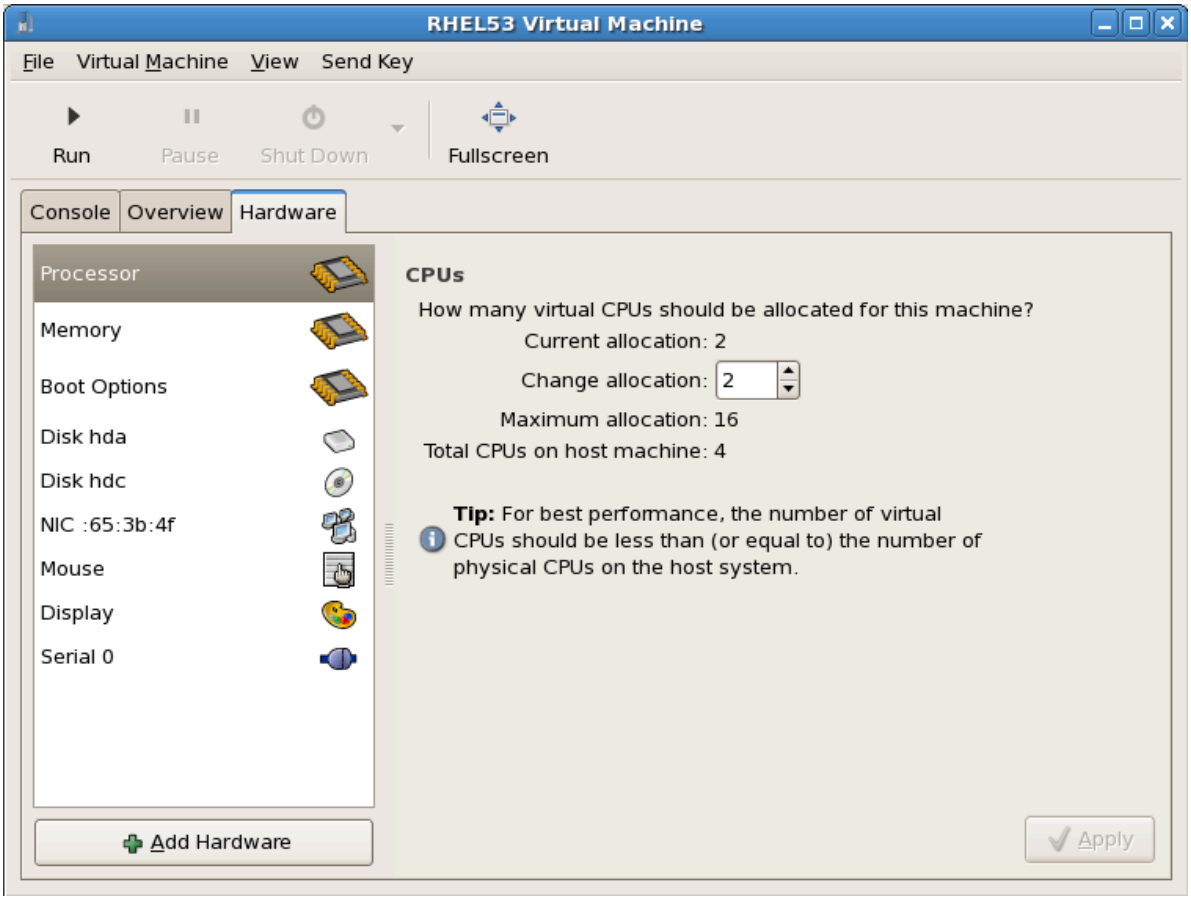


Figura 29.12. Panel de asignación del procesador

5. En la pestaña **Hardware**, haga clic en **Memoria** para ver o modificar la asignación de memoria RAM actual.

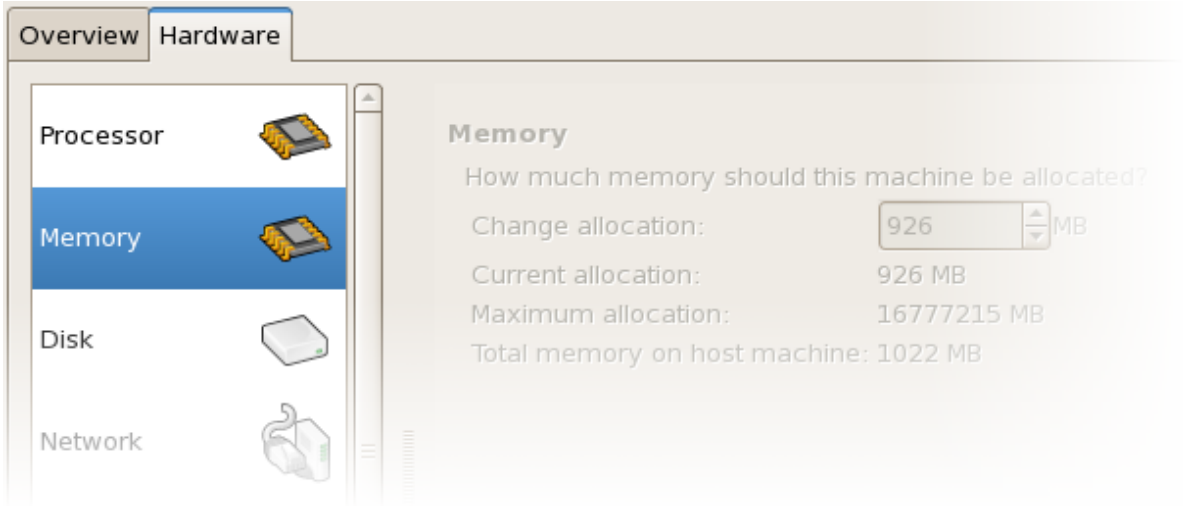


Figura 29.13. Mostrar asignación de memoria

6. En la pestaña **Hardware**, haga clic en **Disco** para ver o cambiar la configuración del disco duro actual.

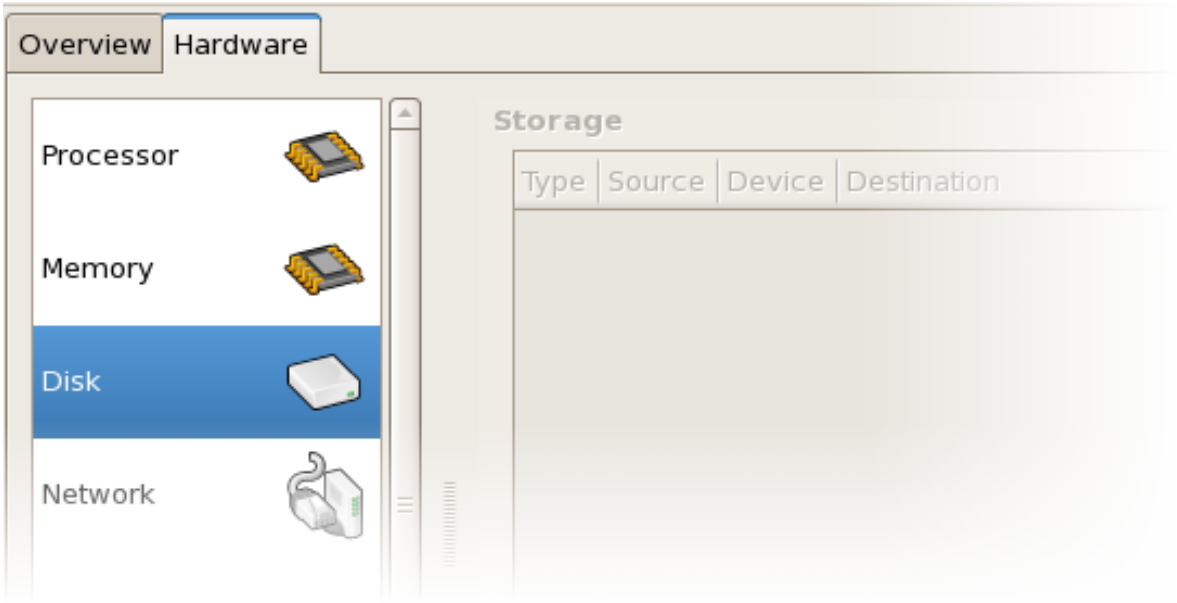


Figura 29.14. Mostrar configuración del disco

7. En la pestaña **Hardware**, haga clic en **Red** para ver o cambiar la configuración de red actual.

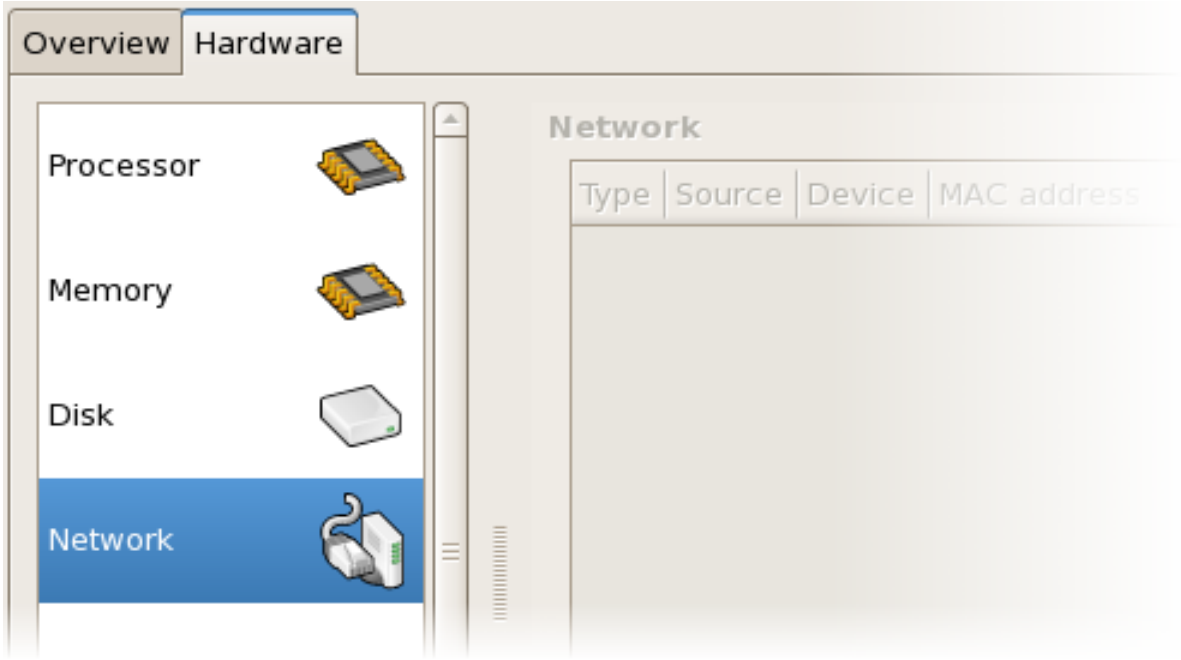


Figura 29.15. Mostrar configuración de red

29.8. Estado de monitorización

Status status monitoring preferences can be modified with **`virt-manager`**'s preferences window.

Para configurar el estado de monitorización:

1. Desde el menú **Editar**, seleccione **Preferencias**.

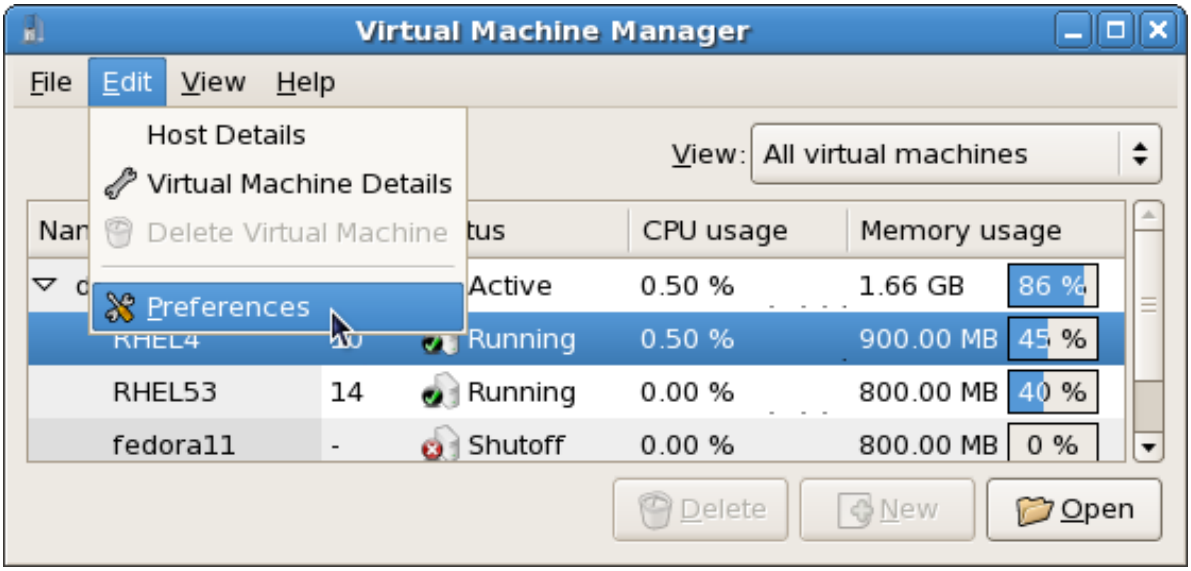


Figura 29.16. Modificar las preferencias del huésped

Aparece la ventana de **Preferencias** aparece.

2. Desde la pestaña **Estadísticas** indique el tiempo en segundos o las opciones de las estadísticas de las consultas.

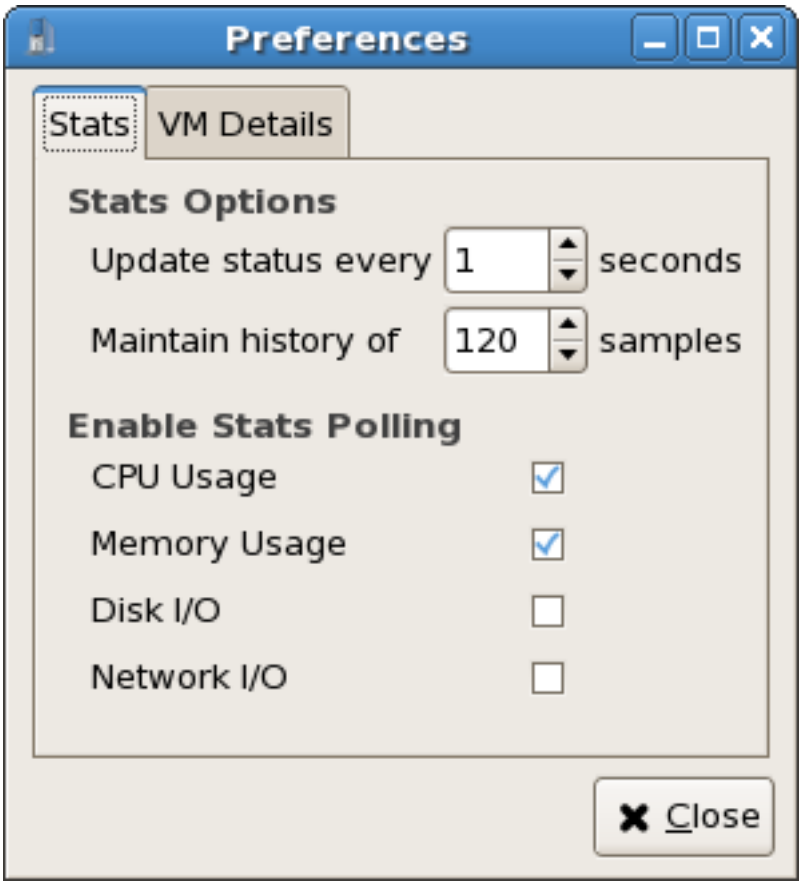


Figura 29.17. Configurar estado de monitorización

29.9. Mostrar los identificadores de huésped

Para ver todos los ID de huésped de todas las máquinas virtuales en su sistema:

1. Desde el menú **Ver**, seleccione la casilla de verificación **ID del dominio**.

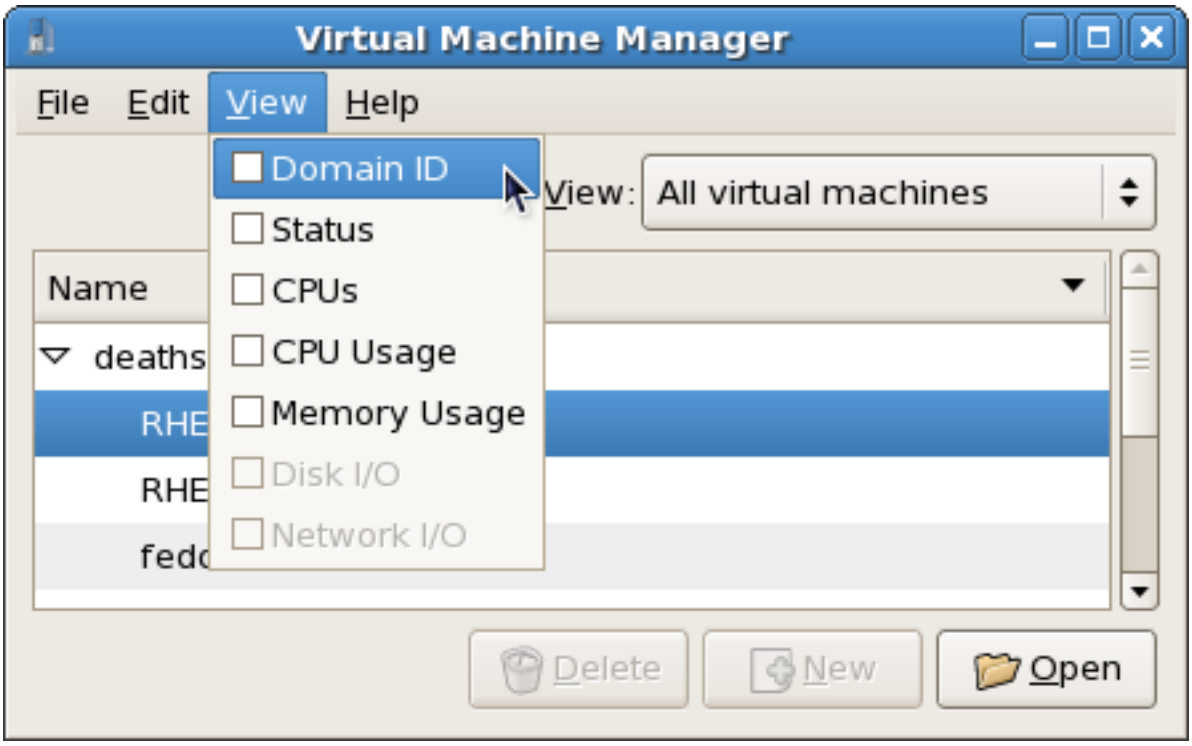


Figura 29.18. Ver ID de huéspedes

2. El Administrador de máquinas virtuales lista todos los ID de dominio para todos los dominios en su sistema.

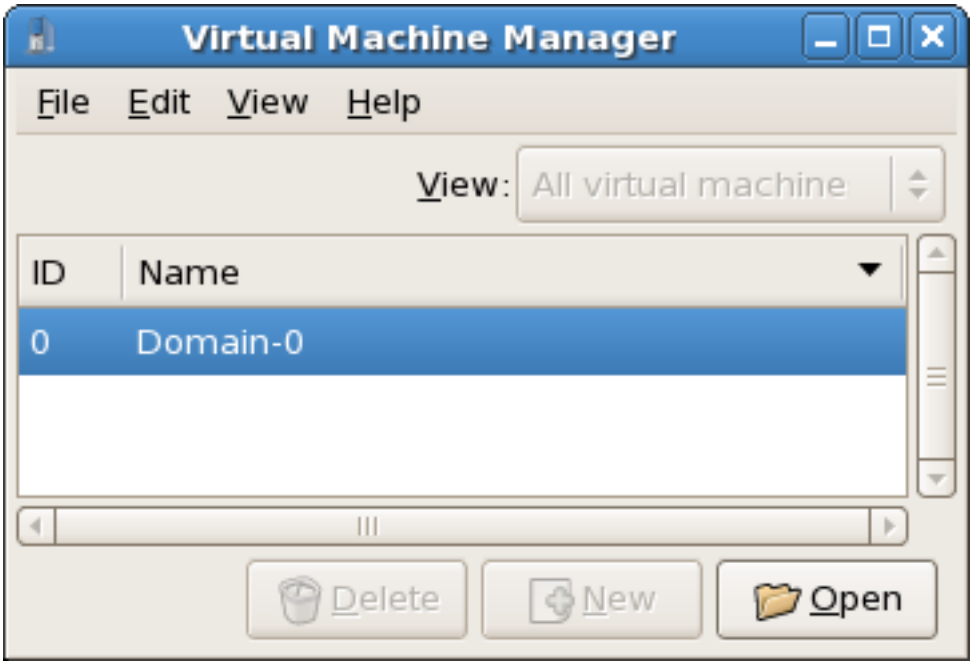


Figura 29.19. Mostrar las ID de dominio

29.10. Displaying a guest's status

Para ver el estado de todas las máquinas virtuales en su sistema:

1. Desde el menú **Ver**, seleccione la casilla de verificación **Estado**.

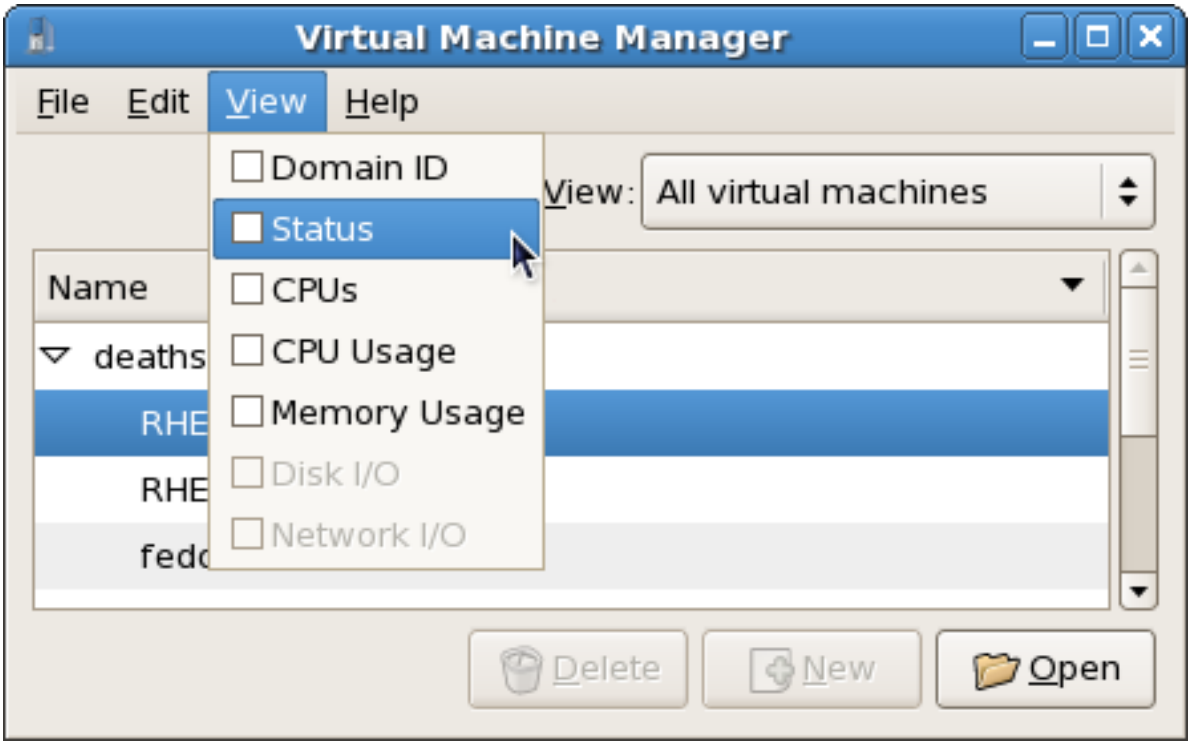


Figura 29.20. Selecting a virtual machine's status

2. El administrador de máquinas virtuales lista el estado de todas las máquinas virtuales en su sistema.

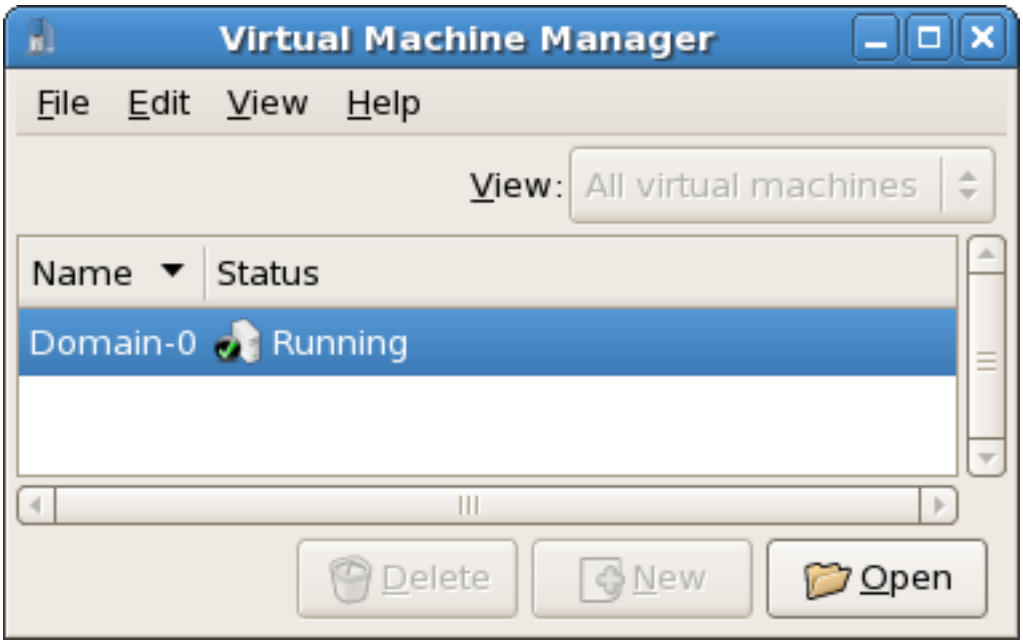


Figura 29.21. Displaying a virtual machine's status

29.11. Mostrar las CPU virtuales

Para ver la cantidad de CPU virtuales para todas las máquinas virtuales en su sistema:

1. Desde el menú **Ver**, seleccione la casilla de verificación **CPU Virtuales**.

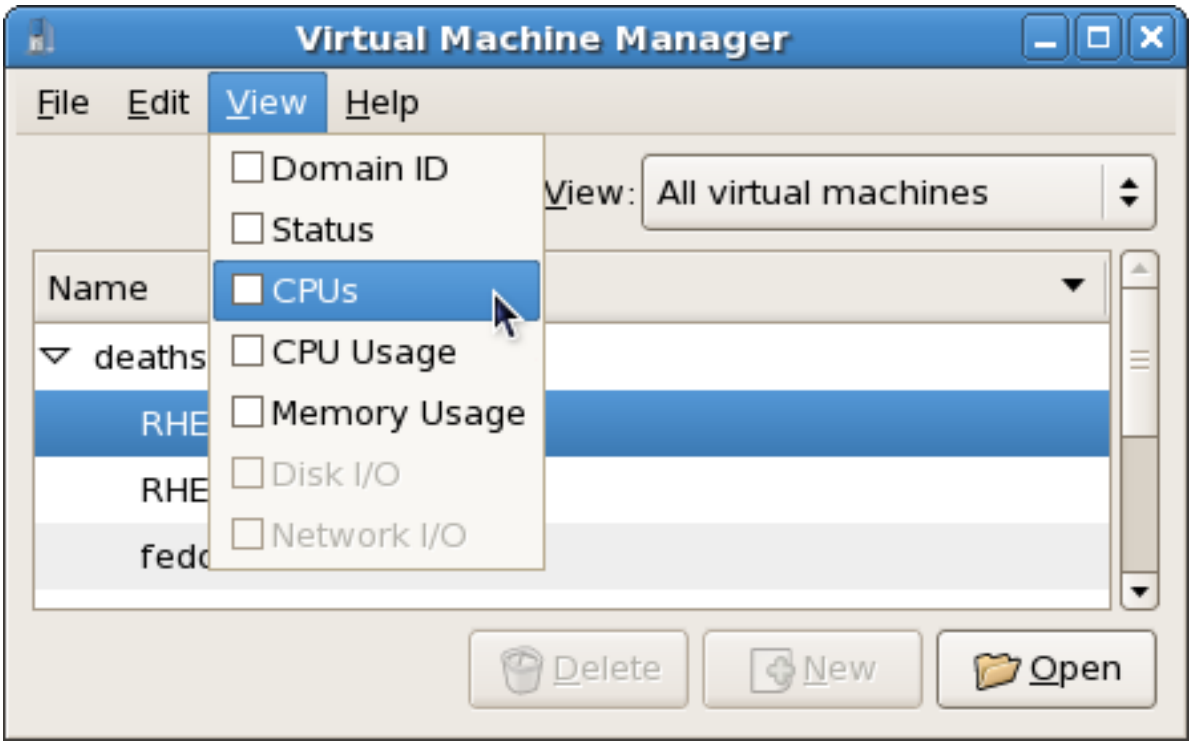


Figura 29.22. Si selecciona la opción de CPU virtuales

2. El administrador de máquinas virtuales lista las CPUs virtuales para todas las máquinas virtuales en su sistema.

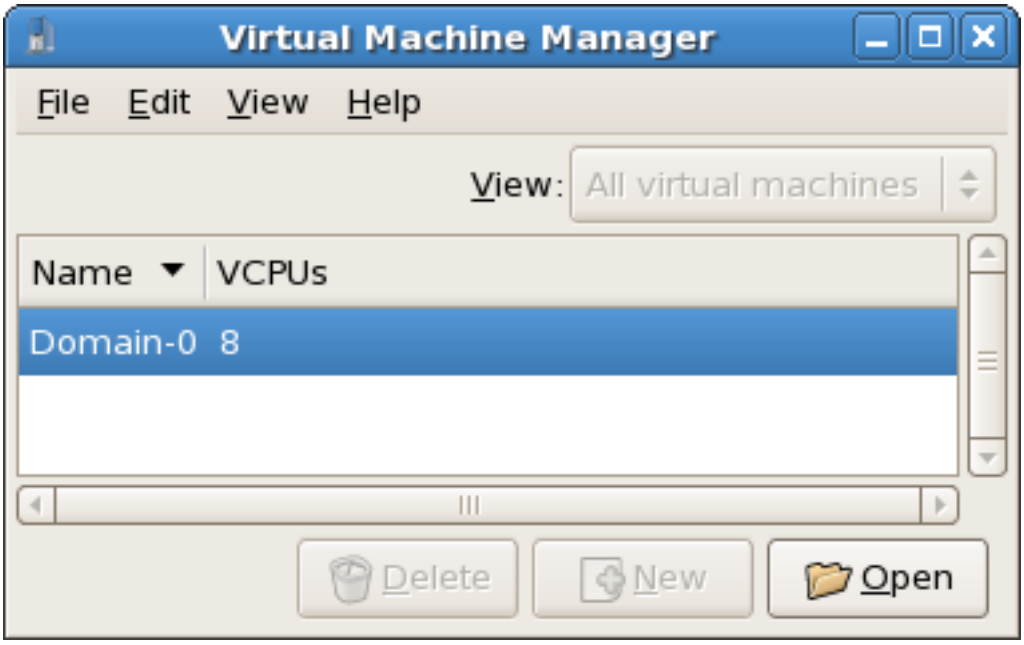


Figura 29.23. Mostrar CPUs virtuales

29.12. Mostrar uso de la CPU

Para ver el uso de CPU para todas las máquinas virtuales en su sistema:

1. Desde el menú **Ver** seleccione **Uso de CPU**

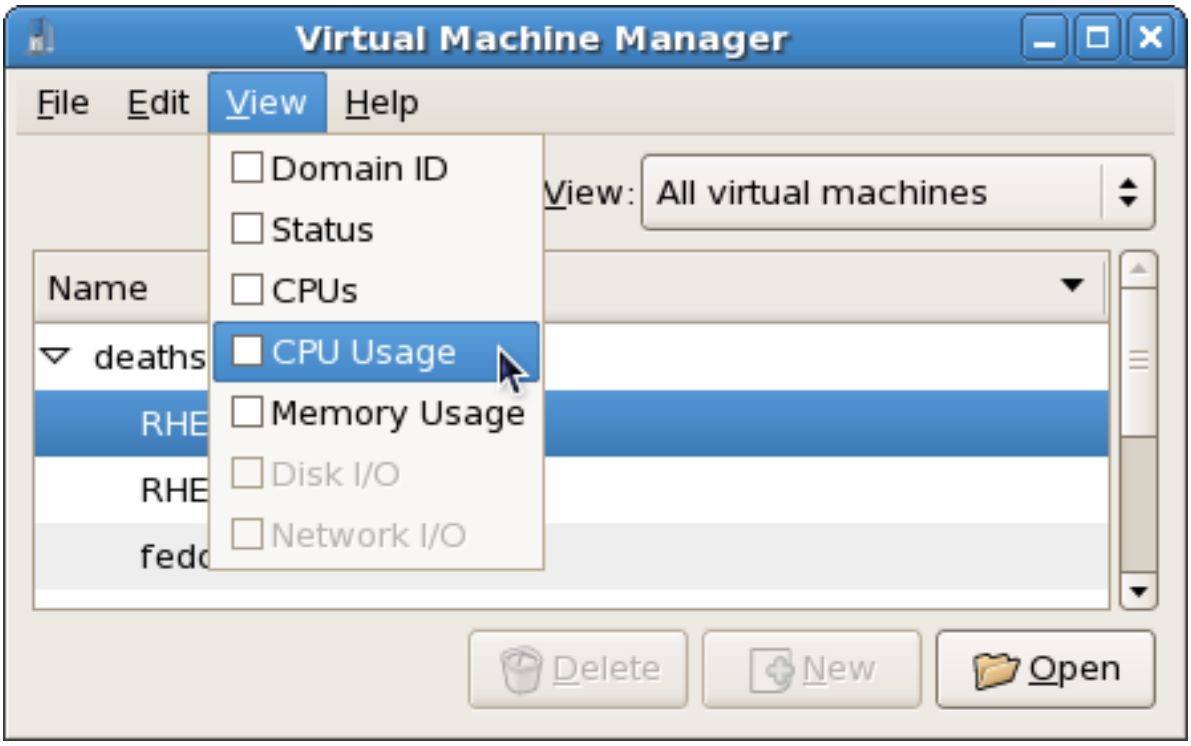


Figura 29.24. Si selecciona el rango DHCP

2. El administrador de máquinas virtuales lista el porcentaje de CPU en uso para todas las máquinas virtuales en su sistema.

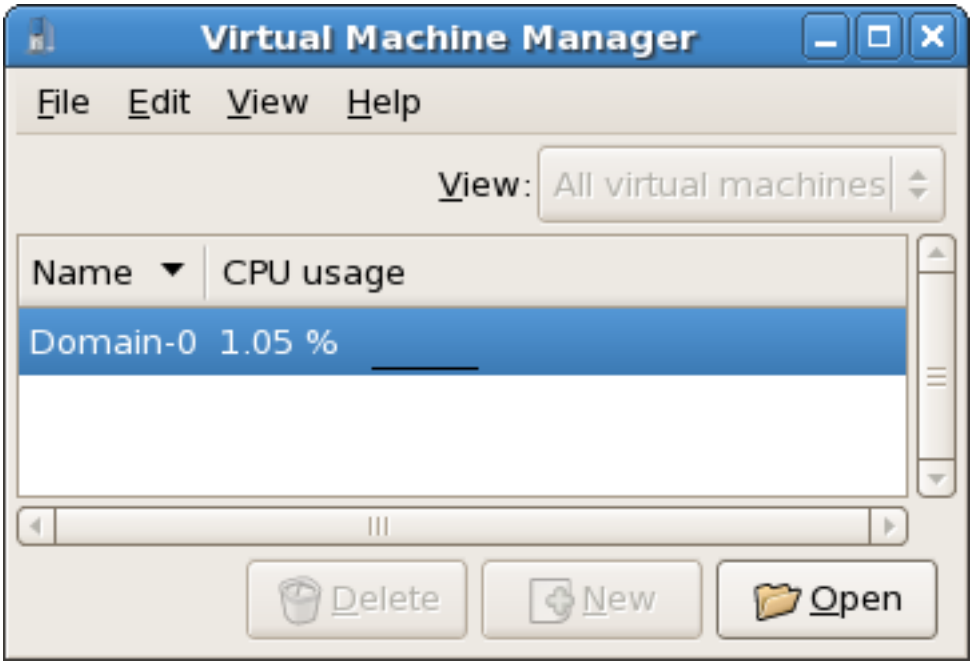


Figura 29.25. Mostrar uso de la CPU

29.13. Mostrar uso de memoria

Para ver el uso de memoria para todas las máquinas virtuales de su sistema:

1. Desde la pestaña **Ver**, seleccione la casilla de verificación **Uso de memoria**.

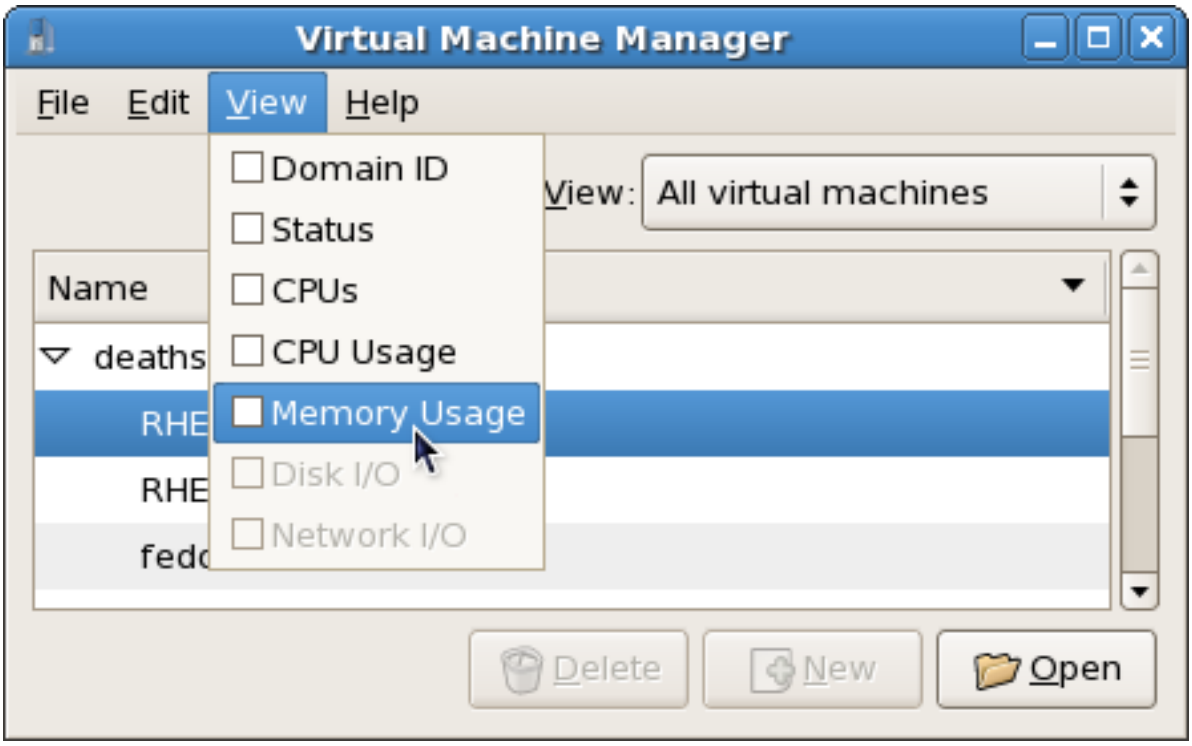


Figura 29.26. Si selecciona uso de memoria

2. El administrador de máquinas virtuales lista el porcentaje de memoria en uso (en megabytes) para todas las máquinas virtuales en su sistema.

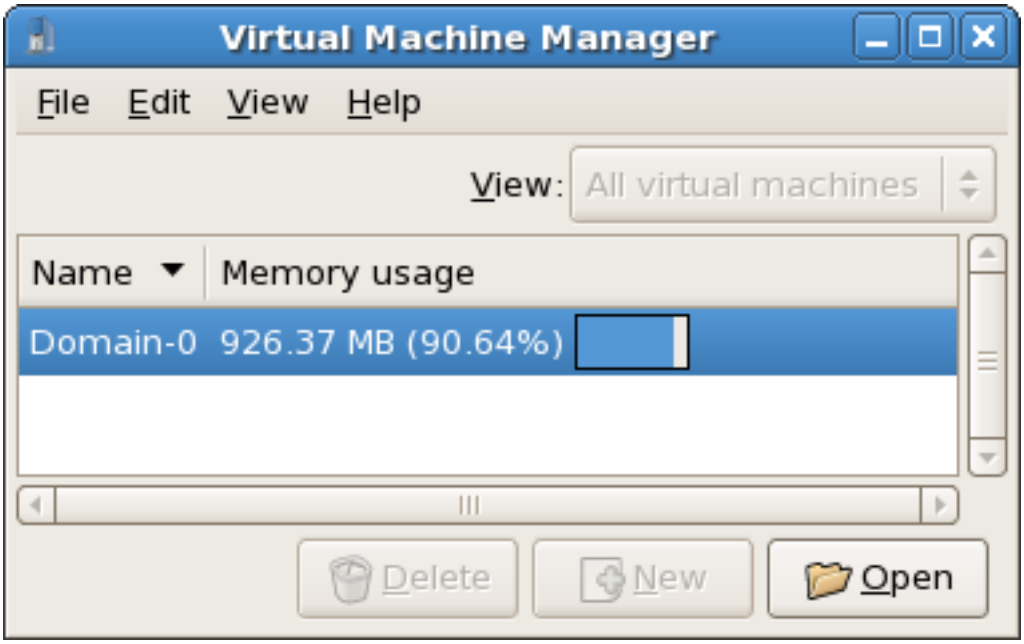


Figura 29.27. Mostrar uso de memoria

29.14. Administración de una red virtual

Para configurar una red virtual en su sistema:

1. Desde el menú **Editar**, seleccione **Detalles del anfitrión**.

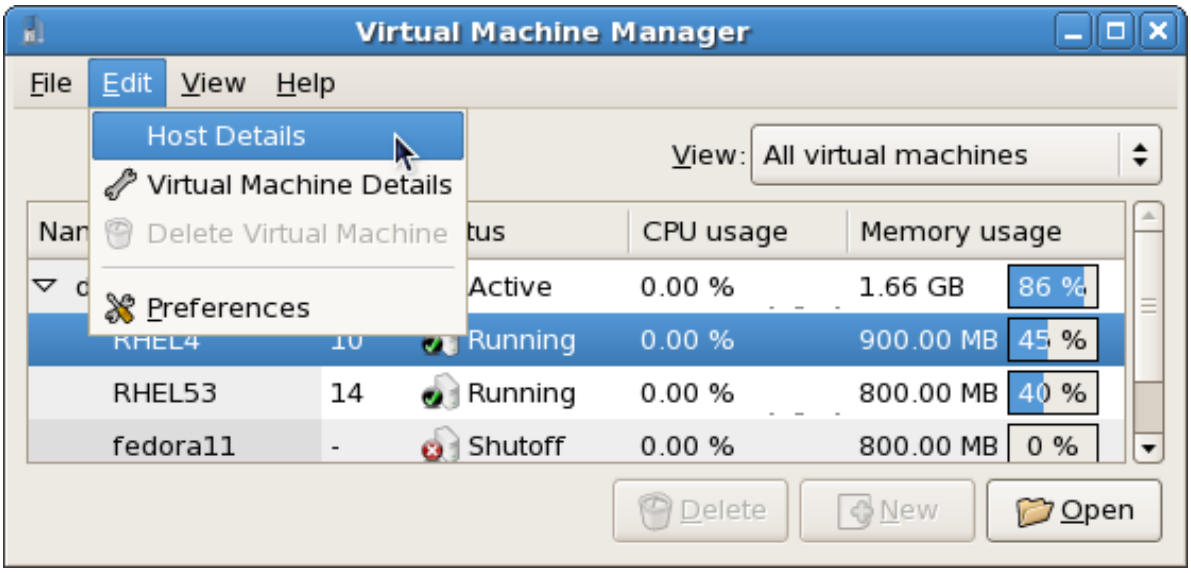


Figura 29.28. Selecting a host's details

2. Se abrirá el menú **Detalles del anfitrión**. Haga clic en la pestaña **Redes virtuales**.

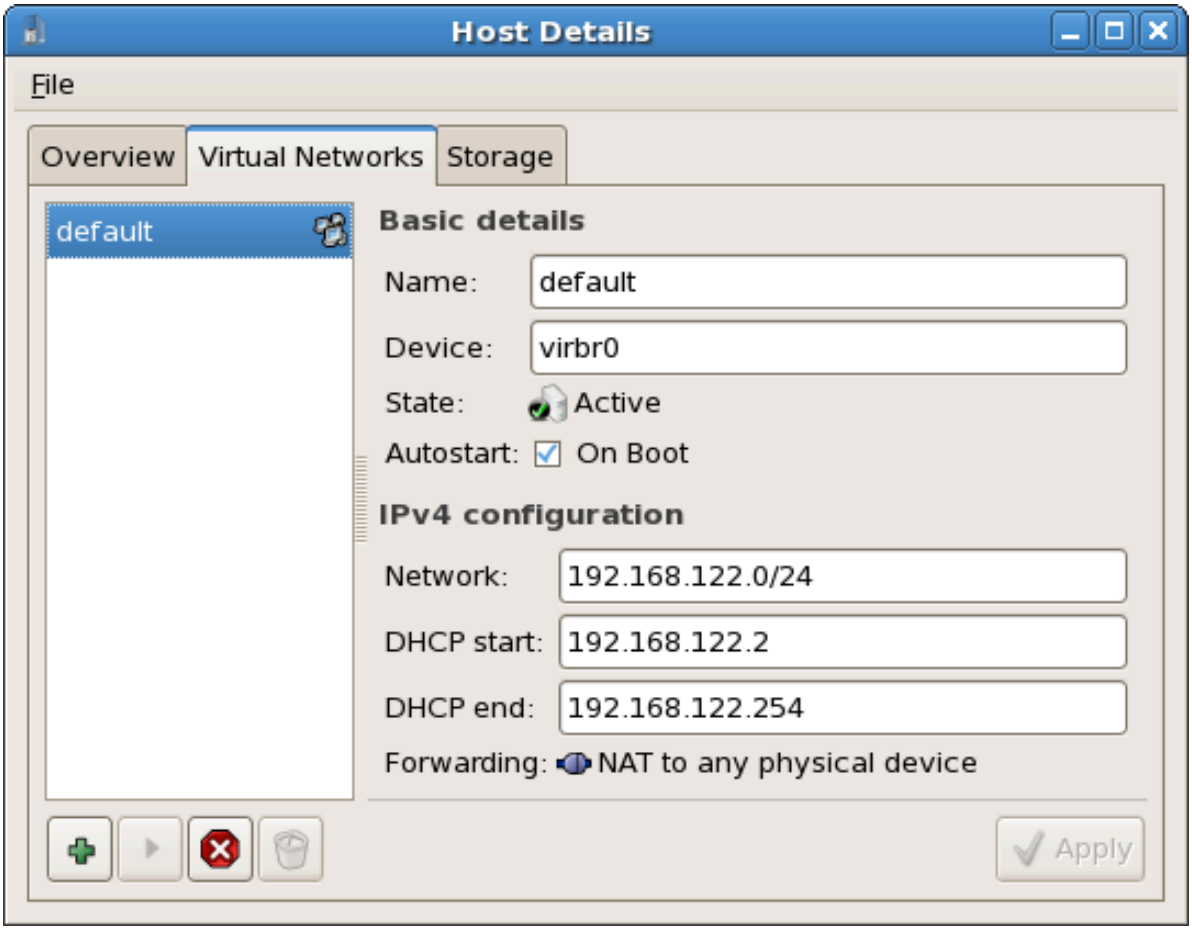


Figura 29.29. Configuración de la red virtual

3. Todas las redes virtuales disponibles se listan en la casilla de la izquierda del menú. Puede editar la configuración de una red virtual seleccionándola en esta casilla y editándola.

29.15. Crear una nueva red virtual

Para crear una red virtual en su sistema:

1. Abra el menú **Detalles del equipo** (consulte *Sección 29.14, “Administración de una red virtual ”*), y haga clic en el botón **Añadir**.

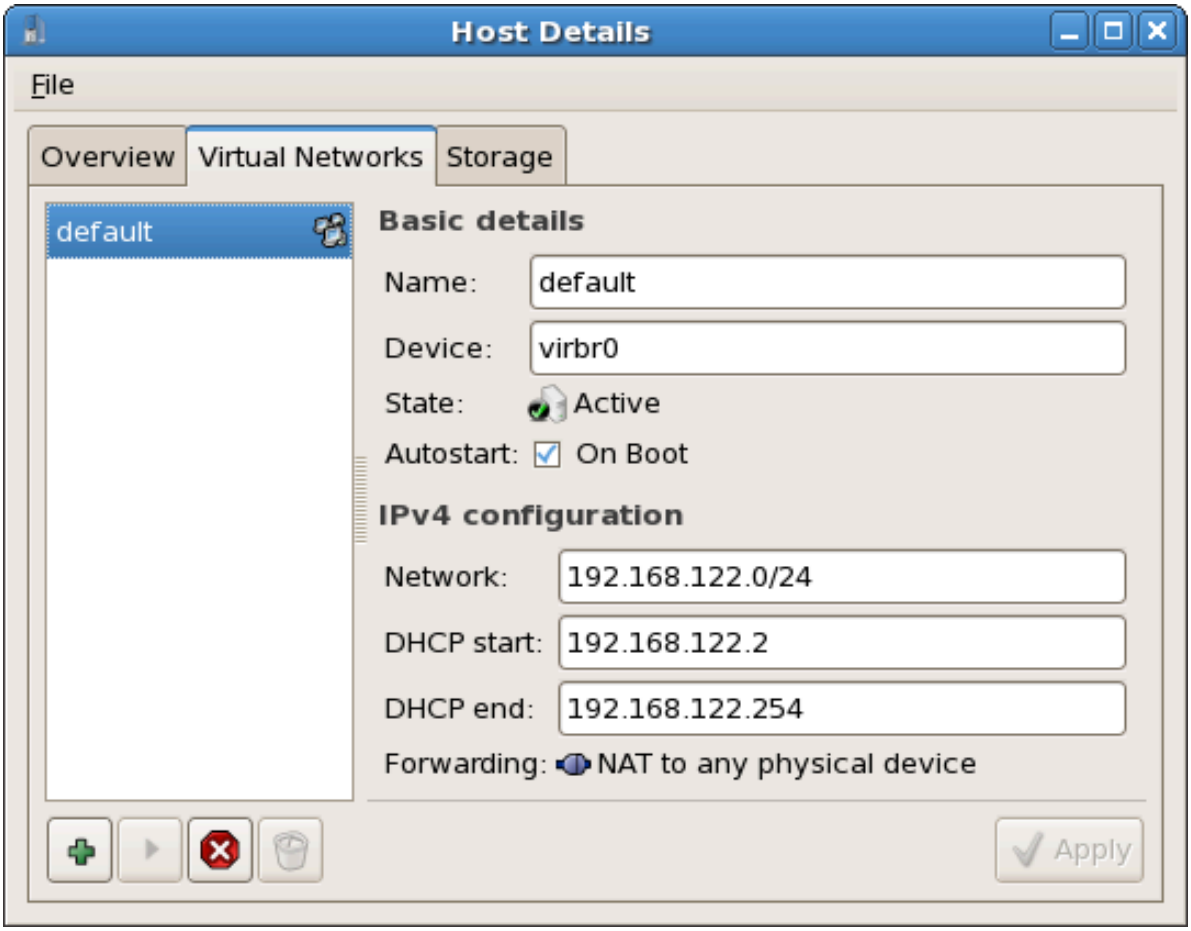


Figura 29.30. Configuración de la red virtual

Se abrirá el menú **Crear una red virtual nueva**. Haga clic en **Adelante** para continuar.

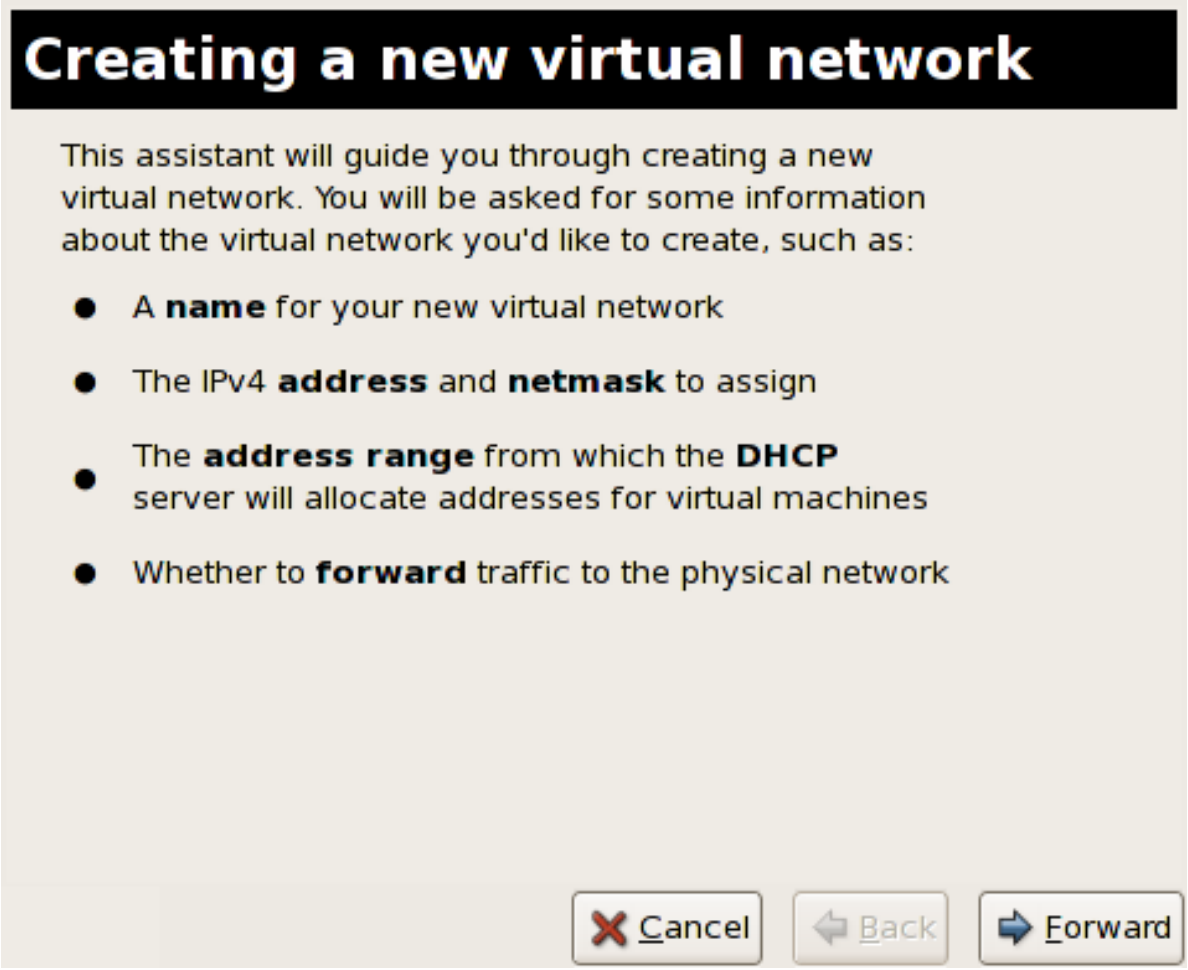

Creating a new virtual network
This assistant will guide you through creating a new virtual network. You will be asked for some information about the virtual network you'd like to create, such as:
A name for your new virtual network
The IPv4 address and netmask to assign
The address range from which the DHCP server will allocate addresses for virtual machines
Whether to forward traffic to the physical network
Cancel
Back
Forward

Figura 29.31. Crear una nueva red virtual

2. Introduzca un nombre apropiado para su red virtual y haga clic en **Adelante**.

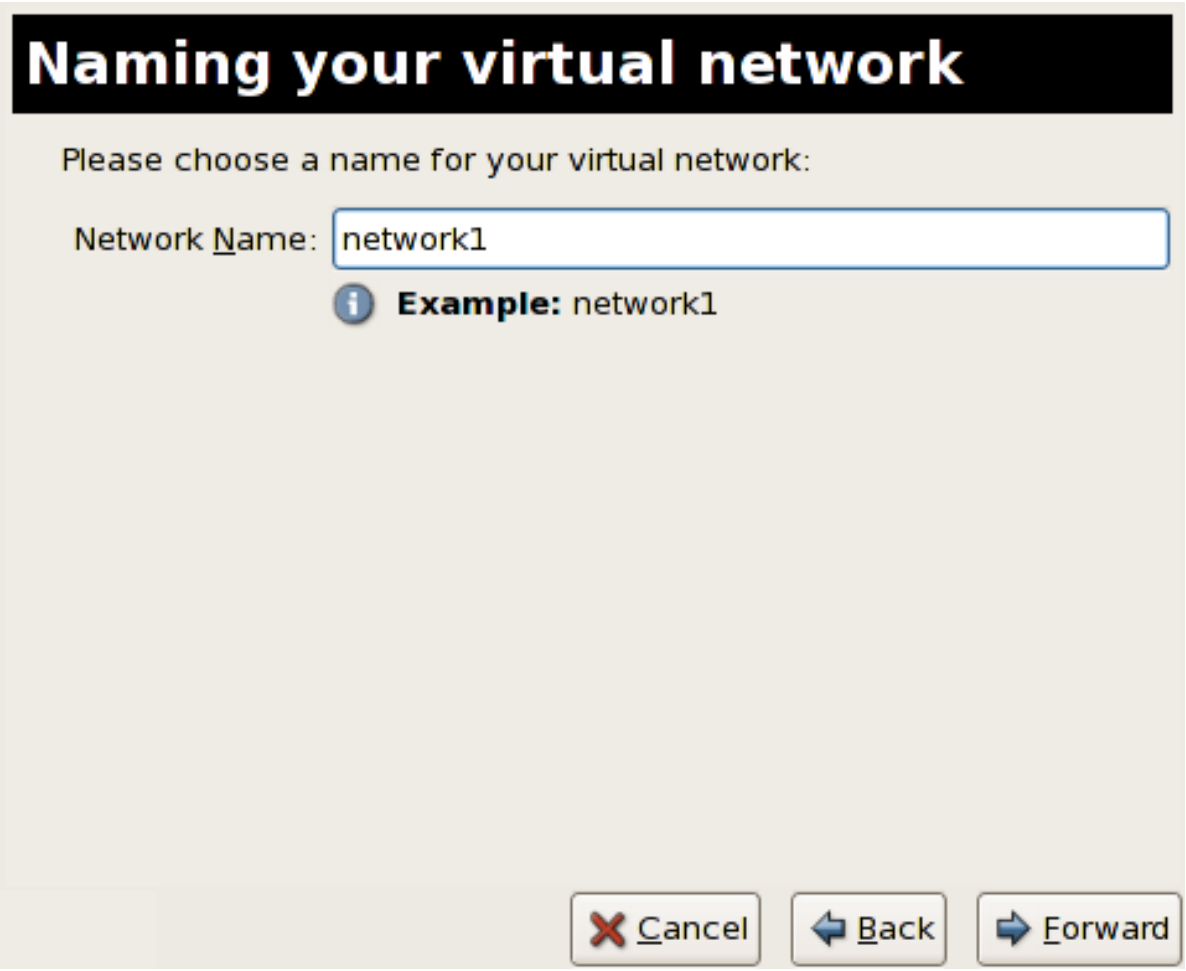


Figura 29.32. Dando un nombre a la red virtual

3. Introduzca un espacio de dirección IPv4 para su red virtual y haga clic en **Adelante**.

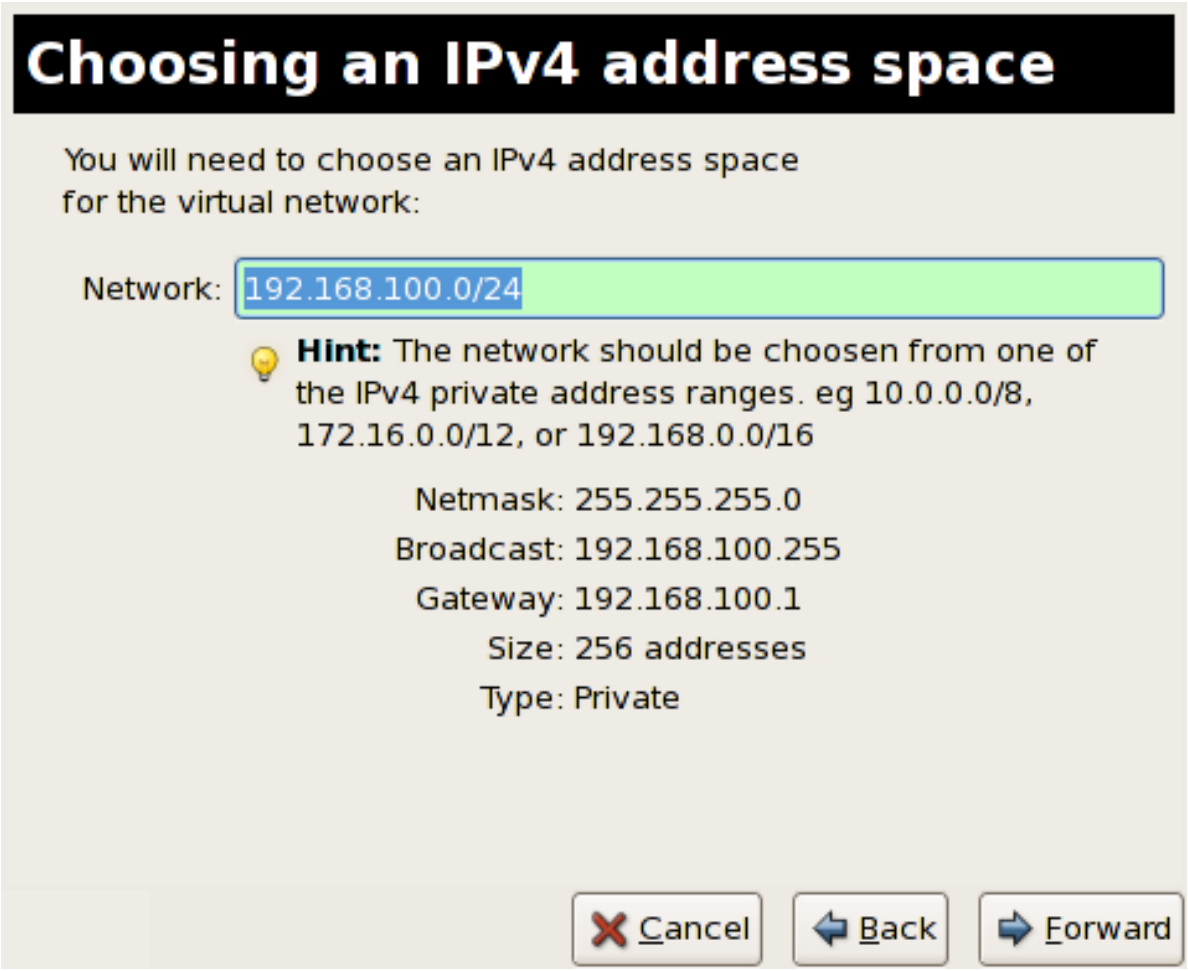

Choosing an IPv4 address space
You will need to choose an IPv4 address space for the virtual network:
Network:
192.168.100.0/24
Hint: The network should be choosen from one of the IPv4 private address ranges. eg 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16
Netmask: 255.255.255.0
Broadcast: 192.168.100.255
Gateway: 192.168.100.1
Size: 256 addresses
Type: Private
Cancel
Back
Forward

Figura 29.33. Selección de un espacio de dirección IPv4

4. Defina el rango DHCP para su red virtual especificando un rango de **Comienzo** y **Fin** de direcciones IP. Haga clic en **Adelante** para continuar.

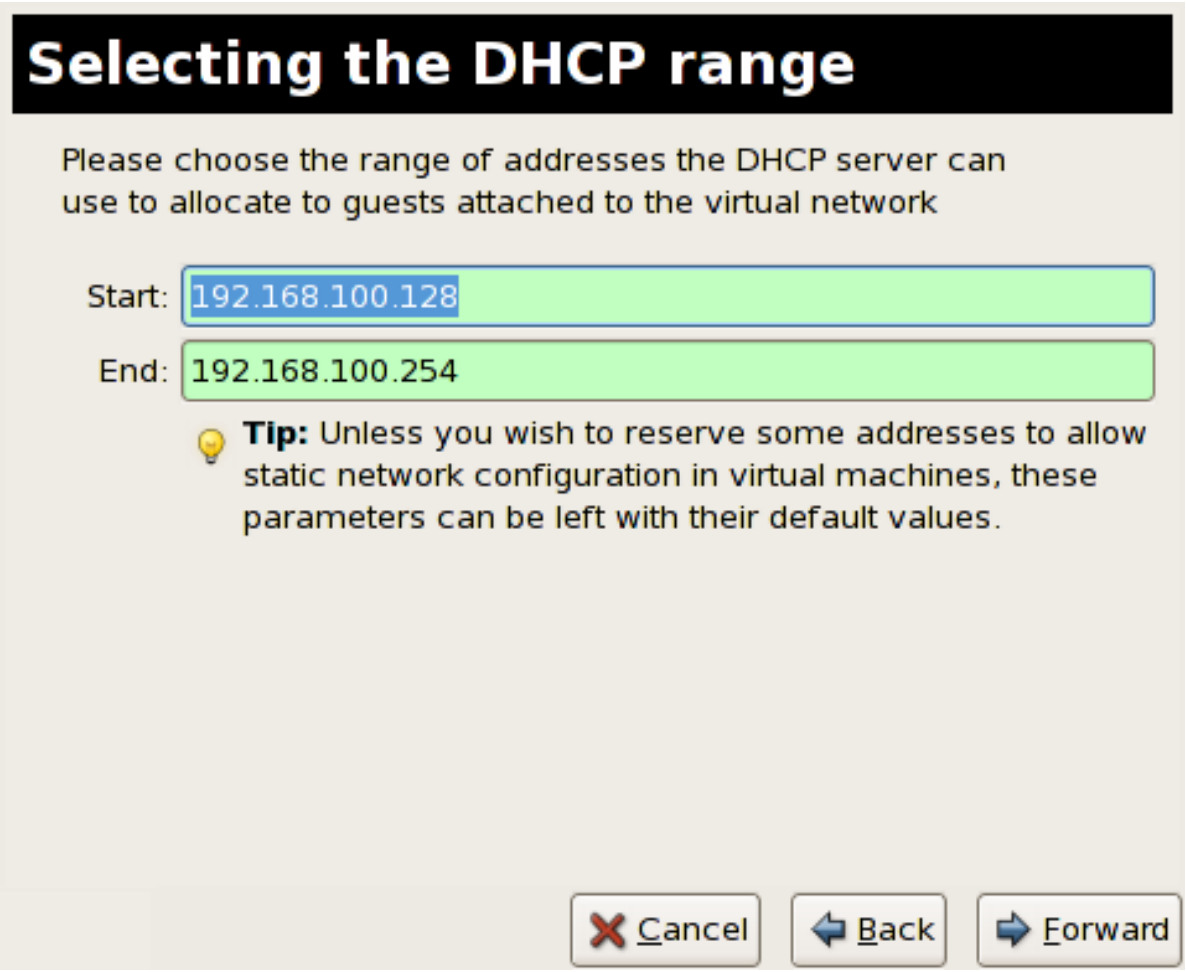

Selecting the DHCP range
Please choose the range of addresses the DHCP server can use to allocate to guests attached to the virtual network
Start:
192.168.100.128
End:
192.168.100.254
Tip: Unless you wish to reserve some addresses to allow static network configuration in virtual machines, these parameters can be left with their default values.
Cancel
Back
Forward

Figura 29.34. Si selecciona el rango DHCP

5. Seleccione cómo la red virtual se debe conectar con la red física.

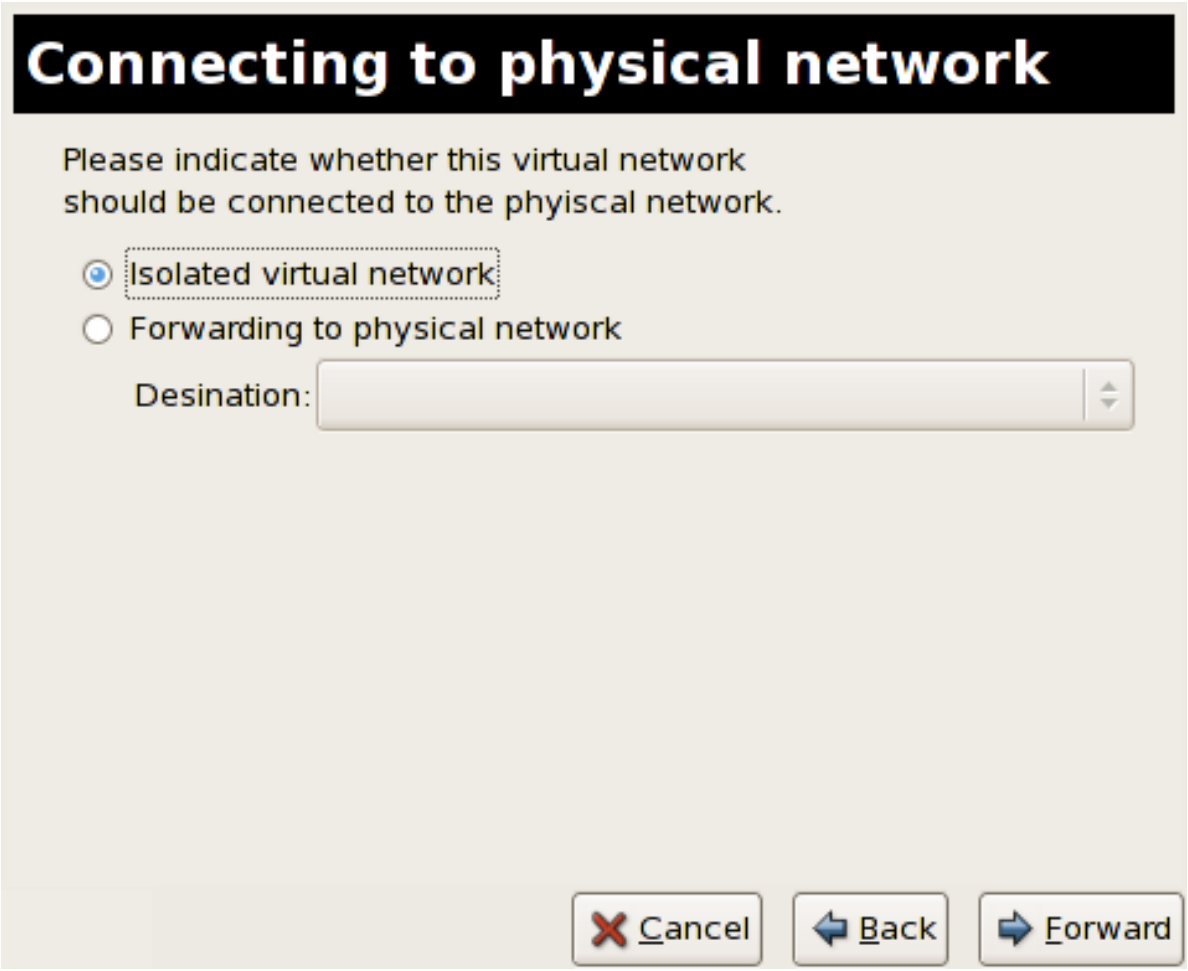


Figura 29.35. Conexión a la red física

Si selecciona **Reenvío a la red física**, seleccione si el **Destino** debe ser **NAT a un dispositivo físico** o **NAT al dispositivo físico eth0**.

Para continuar, haga clic en **Avanzar**.

6. Ahora está listo para crear la red. Revise la configuración de su red y haga clic en **Finalizar**.

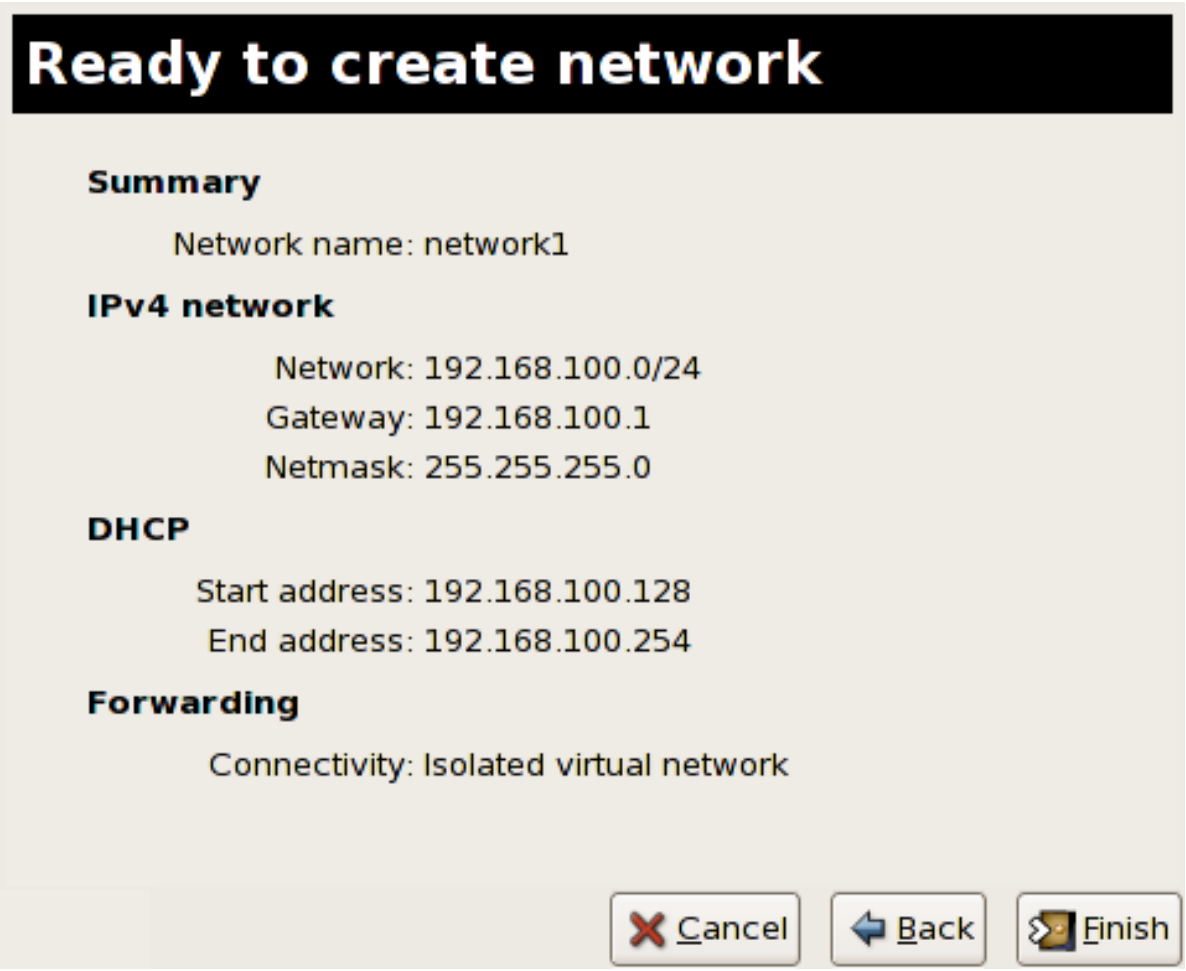


Figura 29.36. Listo para crear la red

7. La nueva red virtual está ya disponible en la pestaña **Red Virtual** del menú **Detalles del anfitrión**.

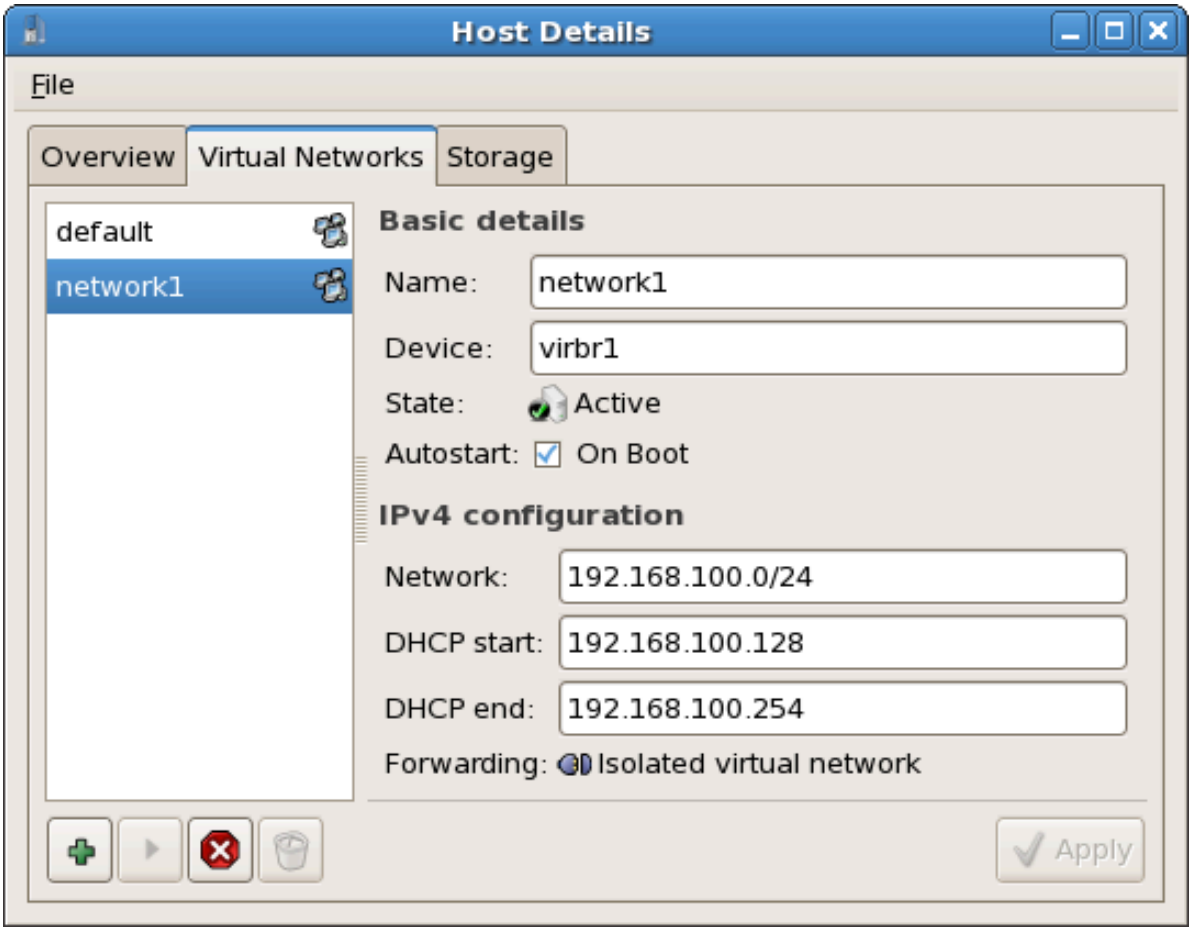


Figura 29.37. La nueva red virtual ya está disponible

referencia de configuración de libvirt

Este capítulo ofrece una referencia a numerosos parámetros de archivos de configuración XML de libvirt

Elemento	Descripción
pae	Especifica los datos de configuración de la extensión de dirección física (PAE, por las iniciales en inglés de Physical Adress Extension).
apic	Especifica los datos de configuración del controlador del interruptor avanzado programable (APIC, por las iniciales en inglés de advanced programmable interrupt controller).
memory	Especifica el tamaño de la memoria en megabytes.
vcpus	Especifica la cantidad de CPUs virtuales.
console	Especifica los números de los puertos a los que exportar las consolas del dominio.
nic	Especifica la cantidad de interfaces de red virtuales.
vif	Lists the randomly-assigned MAC addresses and bridges assigned to use for the domain's network addresses.
disk	Lista los dispositivos de bloque a ser exportados al dominio, y exporta los dispositivos físicos al dominio solo con acceso de lectura.
dhcp	Habilita el entorno de red utilizando DHCP.
netmask	Especifica las máscaras de red IP configuradas.
gateway	Especifica las puertas de enlace IP configuradas.
acpi	Especifica los datos de configuración de la interfaz de configuración avanzada.

Tabla 30.1. archivos de configuración de libvirt

Creación de scripts libvirt personales

Esta sección ofrece información que puede ser útil para programadores y administradores de sistemas que tengan intención de escribir scripts personalizados para hacer sus vidas más cómodas mediante **libvirt**.

Se recomienda la lectura de *Capítulo 25, Tareas de administración diversas* a todos aquellos programadores que estén pensando en escribir aplicaciones nuevas que utilicen **libvirt**.

31.1. Uso de los archivos de configuración XML con virsh

virsh puede manejar los archivos de configuración XML. Puede utilizarlo como una ventaja para escribir implementaciones grandes con opciones especiales. Puede agregar dispositivos definidos en un archivo XML a un huésped para-virtualizado que se encuentre en ejecución. Por ejemplo, para añadir un archivo ISO como **hdc** a un huésped en ejecución, cree un archivo XML:

```
# cat satelliteiso.xml
<disk type="file" device="disk">
 <driver name="file"/>
 <source file="/var/lib/libvirt/images/rhn-satellite-5.0.1-11-redhat-linux-as-i386-4-embedded-
oracle.iso"/>
 <target dev="hdc"/>
 <readonly/>
</disk>
```

Run **virsh attach-device** to attach the ISO as **hdc** to a guest called "satellite" :

```
# virsh attach-device satellite satelliteiso.xml
```

Parte VII. Solución de problemas

Introducción a la identificación y solución de problemas

Los siguientes capítulos proporcionan información para ayudarlo a identificar y solucionar problemas que se presentan al utilizar virtualización.

Solución de problemas

Este capítulo cubre problemas comunes y soluciones con virtualización en Fedora.

La intención de este capítulo es la de ofrecerle al lector un contexto para que pueda identificar dónde se encuentran los problemas relacionados con las tecnologías de virtualización. La solución de los dichos problemas requiere práctica y experiencia, y esto es difícil de adquirir simplemente leyendo un libro. Se recomienda la realización de experimentos y de pruebas con tecnologías de virtualización en Fedora, para poder así desarrollar habilidades propias para la solución de los problemas.

Si no puede encontrar una respuesta en este documento, podría existir una en línea, ofrecida por la comunidad de virtualización. Diríjase a *Sección A.1, “Recursos en línea”* para conocer una lista conteniendo sitios relacionados con la virtualización.

32.1. Herramientas de depuración, y de solución de problemas

La presente sección resume las aplicaciones de Administrador de Sistemas, las utilidades de red, y las herramientas de depuración. Puede utilizar estas herramientas predeterminadas de Administración de sistemas, y conocer los registros para orientarlo en la sosulicón de los problemas:

- **`vmstat`**
- **`iostat`**
- **`lsof`**
- **`systemtap`**
- **`crash`**
- **`sysrq`**
- **`sysrq t`**
- **`sysrq w`**

Estas herramientas de red pueden asisitirlo en la solución de problemas relacionados con el entorno de red de una virtualización:

- **`ifconfig`**
- **`tcpdump`**

  The **`tcpdump`** command 'sniffs' network packets. **`tcpdump`** is useful for finding network abnormalities and problems with network authentication. There is a graphical version of **`tcpdump`** named **`wireshark`**.

- **`brctl`**

  `brctl` es una herramienta de red que inspecciona y configura el puente Ethernet en el Kernel Linux de una virtualización. Debe tener acceso de usuario root antes de ejecutar los comandos siguientes:

```
# brctl show
bridge-name    bridge-id          STP  enabled  interfaces
-----------------------------------------------------------------------------
virtbr0             8000.fefffff       yes        eth0

# brctl showmacs virtbr0
port-no           mac-addr                  local?       aging timer
1                 fe:ff:ff:ff:ff:           yes            0.00
2                 fe:ff:ff:fe:ff:           yes            0.00
# brctl showstp virtbr0
virtbr0
bridge-id              8000.feffffffff
designated-root        8000.feffffffff
root-port              0                   path-cost             0
max-age                20.00               bridge-max-age        20.00
hello-time             2.00                bridge-hello-time     2.00
forward-delay          0.00                bridge-forward-delay  0.00
aging-time            300.01
hello-timer            1.43                tcn-timer             0.00
topology-change-timer  0.00                gc-timer              0.02
```

A continuación ofrecemos otro listado con comandos útiles para la solución de problemas relacionados con la virtualización.

- **strace** es un comando que rastrea las llamadas del sistema, y los eventos recibidos y utilizados por otro proceso.
- **vncviewer**: se conecta a un servidor VNC ejecutándose en su servidor o en una máquina virtual. Instale **vncviwer** utilizando el comando **`yum install vnc`**.
- **vncserver**: inicia un escritorio remoto en su servidor. Le ofrece la posibilidad de ejecutar interfaces de usuarios gráficas, como ser por ejemplo virt-manager a trevés de una sesión remota. Instale **vncserver** utilizando el comando **`yum install vnc-server`**.

32.2. Archivos de registro

KVM utiliza numerosos archivos de registro. Todos los archivos de registro son archivos ASCII estándar, y puede accederse a ellos con un editor de textos.

- El directorio predeterminado para todas las imagenes basadas en arcvhivos es el directorio **`/var/lib/libvirt/images`**.
- **`qemu-kvm.[PID].log`** es el archivo de registro creado por el proceso **`qemu-kvm`** para cada huésped totalmente virtualizado. Cuando se utilice este archivos, debe recuperar el proceso PID ofrecido por **`qemu-kvm`**, utilizando el comando **`ps`** para examinar los argumentos del proceso, y de esta manera aislar los procesos **`qemu-kvm`** de la máquina virtual. Tenga en cuenta que debe reemplazar el simbolo [PID] con el actual proceso PID **`qemu-kvm`**.

Si encuentra algún tipo de error con el Administrador de máquinas virtuales, puede revisar los datos generados en el archivo **`virt-manager.log`**, dentro del directorio **`/.virt-manager`** . Tenga en cuenta que cada vez que inicie el Administrador de máquinas virtuales, sobreescribe los contenidos del archivo de registro existente. Asegúrese de realizar un respaldo del archivo **`virt-manager.log`** , antes de reiniciar el Administrador de máquinas virtuales luego de un error del sistema.

32.3. Solución de problemas con consolas seriales

Los diversos Kernels de Linux pueden ofrecer información para los puertos seriales. Esto es útil para depurar los denominados "kernel panics" y los problemas relacionados con el hardware de los dispositivos de video o servidores ciegos. Las subsecciones de esta sección describen cómo configurar una salida de consola serial para máquinas ejecutando kernels de virtualización en Fedora, y sus respectivos huéspedes virtualizados.

La presente sección detalla cómo habilitar la salida de consolas seriales para huéspedes completamente virtualizados.

La salida de consola serial de un huésped completamente virtualizado puede ser observada con el comando **`virsh console`**.

Tenga en cuenta que las consolas seriales de los huéspedes completamente virtualizados poseen algunas limitaciones. Hoy en día, algunas de estas limitaciones son:

- los datos de salida podrían ser interrumpidos o mezclados.

El puerto serial es denominado `ttyS0` en Linux, o `COM1` en Windows.

Debe configurar el sistema operativo virtualizado para ofrecer información al puerto serial virtual.

Para poder ofrecer información del kernel de un huésped Linux completamente virtualizado hacia el dominio, modifique el archivo **`/boot/grub/grub.conf`**, agregándole la línea *`console=tty0 console=ttys0,115200`*.

```
title Fedora Server (2.6.18-92.el5)
 root (hd0,0)
 kernel /vmlinuz-2.6.18-92.el5 ro root=/dev/volgroup00/logvol00
 console=tty0 console=ttys0,115200
 initrd /initrd-2.6.18-92.el5.img
```

Reinicie el huésped.

En el equipo, ingrese a la consola serial con el siguiente comando:

```
# virsh console
```

Además, puede utilizar **`virt-manager`** para observar la consola de texto virtual. En la ventana de consola del huésped, seleccione **Consola serial** desde el menú **Ver**.

32.4. Archivos de registro de virtualización

- /var/log/libvirt/qemu/*`GuestName`*.log

Si encuentra algún tipo de error con el Administrador de máquinas virtuales, puede revisar los datos generados en el archivo **`virt-manager.log`**, dentro del directorio **`/.virt-manager`** . Tenga en cuenta que cada vez que inicie el Administrador de máquinas virtuales, sobreescribe los contenidos del archivo de registro existente. Asegúrese de realizar un respaldo del archivo **`virt-manager.log`** , antes de reiniciar el Administrador de máquinas virtuales luego de un error del sistema.

32.5. Errores del dispositivo en bucle

Si se utilizan imágenes basadas en archivos, tal vez deba aumentar el número de dispositivos de bucle configurados. La configuración predeterminada permite hasta ocho dispositivos de bucle. Si se necesitan más de ocho huéspedes basados en archivos, o dispositivos de bucle, puede ajustar la cantidad en el archivo **`/etc/modprobe.conf`**. Edite el archivo **`/etc/modprobe.conf`** y añádale la siguiente línea:

```
options loop max_loop=64
```

Este ejemplo utiliza 64 pero se puede especificar otro número como el máximo valor de bucle. También tendrá que implementar huéspedes respaldados por dispositivos de bucle en su sistema. Para emplear huéspedes de dispositivo de bucle para un huésped para-virtualizado, utilice los comandos **`phy: block device`** o **`tap:aio`**. Para emplear huéspedes respaldados de dispositivo de bucle para un sistema completamente virtualizado, utilice los comandos **`phy: device`** o **`file: file`**.

32.6. Habilitando las extensiones de virtualización de hardware Intel VT y AMD-V en BIOS

Esta sección describe cómo identificar extensiones de virtualización de hardware y habilitarlas en su BIOS si están desactivadas.

Las extensiones Intel VT pueden ser inhabilitadas en el BIOS. Algunos proveedore de portátiles tienen extensiones de Intel VT inhabilitadas por defecto en sus CPU.

Las extensiones de virtualización no pueden desactivarse en el BIOS para AMD-V.

Las extensiones de virtualización algunas veces son desactivadas en el BIOS, por lo general por los fabricantes de portátiles. Consulte la Refer to *Sección 32.6, “Habilitando las extensiones de virtualización de hardware Intel VT y AMD-V en BIOS”* para obtener instrucciones sobre cómo habilitar las extensiones de virtualización desactivadas.

Verifique las extensiones de virtualización que están habilitadas en BIOS. Las configuraciones de BIOS para Intel® VT o AMD-V suelen estar en los menús **Chipset** o **Procesador**. Los nombres de menú pueden variar en esta guía, las configuraciones de extensión de virtualización se pueden encontrar en **Configuración de seguridad** u otros nombres usuales de menú.

Procedimiento 32.1. Habilitar extensiones de virtualización en BIOS

1. Reboot the computer and open the system's BIOS menu. This can usually be done by pressing the **delete** key, the **`F1`** key or **`Alt`** and **`F4`** keys depending on the system.

2. Seleccione **Restaurar predeterminados** o **Resturar predeterminados optimizados**, y luego seleccione **Guardar & Salir**.

3. Apague la máquina y desconecte la fuente de energía.

4. **Habilitar las extensiones de virtualización en el BIOS**

Nota: etapas del BIOS

Many of the steps below may vary depending on your motherboard, processor type, chipset and OEM. Refer to your system's accompanying documentation for the correct information on configuring your system.

   a. Prenda la máquina y abra el BIOS (como lo hizo para el paso 1).

   b. Abra el submenú **Procesador**. El menú de configuración del procesador podría estar escondido bajo los menúes **Chipset**, **Configuración avanzada del CPU** o **Northbridge**.

   c. Habilite las opciones **Tecnología de Virtualization Intel** (también conocida como Intel VT), o **AMD-V**, de acuerdo a la marca del procesador. Las extensiones de virtualización pueden encontrarse etiquetadas como **Extensiones de Virtualización**, **Vanderpool**, u otros, de acuerdo al OEM y al BIOS del sistema.

   d. Habilite VTd o AMD IOMMU, si es que estas opciones se encuentran disponibles. Intel VTd y AMD IOMMU son utilizadas para *PCI passthrough*.

   e. Seleccione **Guardar & Salir**.

5. Apague la máquina y desconecte la fuente de energía.

6. Ejecute **`cat /proc/cpuinfo | grep vmx svm`**. Si el comando entrega salida, las extensiones de virtualización ahora están habilitadas. Si no hay salida, puede que su sistema no tenga extensiones de virtualización o el BIOS configurado correcto habilitado.

32.7. Desempeño del entorno de red de KVM

Por defecto, a las máquinas virtuales KVM se les asigna como NIC (controlador de interfaz de red), a un Realtek virtual 8139 (rtl8139).

El NIC virtualizado rtl8139 funciona perfecto en la mayoría de los entornos. Sin embargo, este dispositivo puede sufrir una disminución de su desempeño cuando se lo utilice en algunas redes, como por ejemplo, en una red Ethernet de 10 Gigabit.

Una solución improvisada es la de cambiarlo a una NIC virtualizada de distinto tipo. Por ejemplo, Intel PRO/1000 (e1000) o virtio (el controlador de red paravirtualizado).

Para cambiar al controlador e1000:

1. Apague el sistema operativo huésped.

2. Edit the guest's configuration file with the **`virsh`** command (where *`GUEST`* is the guest's name):

```
# virsh edit GUEST
```

   El comando **`virsh edit`** utiliza la variable de shell **`$EDITOR`** para poder determinar qué editor utilizará.

3. Encuentre la sección de la interfaz de red de la configuración. Esta sección se asemeja a la que mostramos a continuación:

```
<interface type='network'>
  [output truncated]
  <model type='rtl8139' />
</interface>
```

4. Change the type attribute of the model element from *'rtl8139'* to *'e1000'*. This will change the driver from the rtl8139 driver to the e1000 driver.

```
<interface type='network'>
  [output truncated]
  <model type='e1000' />
</interface>
```

5. Guarde las modificaciones y cierre el editor de textos

6. Reinicie el sistema operativo huésped.

De manera alternativa, puede instalar nuevos huéspedes virtualizados con un controlador de red distinto. Esto podría ser necesario si está teniendo dificultades instalando huéspedes sobre una conexión de red. Este método necesita por lo menos ya posea creada una máquina virtual (posiblemente instalada desde un CD o un DVD) para utilizarla como modelo.

1. Genere un XML modelo a partir de una máquina virtual existente:

```
# virsh dumpxml GUEST > /tmp/guest.xml
```

2. Copie y edite el archivo XML y actualice los campos que en él existan: el nombre de la máquina virtual, UUID, imagen de disco, dirección MAC, y demás parámetros. Tenga en cuenta que puede eliminar las líneas correspondientes a la dirección MAC y al UUID, y que virsh generará nuevas.

```
# cp /tmp/guest.xml /tmp/new-guest.xml
# vi /tmp/new-guest.xml
```

   Agregue la línea del modelo en la sección de interfaz de red:

```
<interface type='network'>
  [output truncated]
  <model type='e1000' />
</interface>
```

3. Cree la nueva máquina virtual:

```
# virsh define /tmp/new-guest.xml
# virsh start new-guest
```

El desempeño de red debería ser mejor con el controlador e1000 o virtio. (*BZ#517181*[1])

[1] https://bugzilla.redhat.com/show_bug.cgi?id=517181

Apéndice A. Recursos adicionales

Para saber más acerca de virtualización y Fedora, consulte alguna de las siguientes opciones:

A.1. Recursos en línea

- *http://www.libvirt.org/* es el sitio Web oficial para API de virtualización de **libvirt**.
- *http://virt-manager.et.redhat.com/* es el proyecto de sitio Web para el **Administrador de máquina virtual** (virt-manager), la aplicación gráfica para máquinas virtuales.
- Centro de virtualización

  http://www.openvirtualization.com[1]
- Documentación de Red Hat

  http://www.redhat.com/docs/
- Vista general de las tecnologías de virtualización

  http://virt.kernelnewbies.org[2]
- Grupo de tecnologías emergentes de Red Hat

  http://et.redhat.com[3]

A.2. Documentación instalada

- **man virsh** and **/usr/share/doc/libvirt-*<version-number>*** — Contains sub commands and options for the **virsh** virtual machine management utility as well as comprehensive information about the **libvirt** virtualization library API.
- **/usr/share/doc/gnome-applet-vm-*<version-number>*** — Documentation for the GNOME graphical panel applet that monitors and manages locally-running virtual machines.
- **/usr/share/doc/libvirt-python-*<version-number>*** — Provides details on the Python bindings for the **libvirt** library. The **libvirt-python** package allows python developers to create programs that interface with the **libvirt** virtualization management library.
- **/usr/share/doc/python-virtinst-*<version-number>*** — Provides documentation on the **virt-install** command that helps in starting installations of Fedora and Red Hat Enterprise Linux related distributions inside of virtual machines.
- **/usr/share/doc/virt-manager-*<version-number>*** — Provides documentation on the Virtual Machine Manager, which provides a graphical tool for administering virtual machines.

Glosario

Este glosario tiene el objetivo de definir los términos que se utilizan en este Manual de instalación.

Anfitrión	El sistema operativo del equipo anfitrión ejecuta huéspedes virtualizados.
Bare-metal	El término bare-metal (vacío) se refiere a la arquitectura física subyacente de una computadora. Ejecutar un sistema operativo en un bare-metal es otra forma de referirse al hecho de ejecutar una versión sin modificar de un sistema operativo en el hardware físico. Un ejemplo la ejecución de un sistema operativo sobre bare-metal, es el sistema operativo instalado normalmente.
Completamente virtualizado	Consulte *Virtualización completa*.
Controladores para-virtualizados	Los controladores para-virtualizados son controladores de dispositivo que operan en huéspedes de Linux completamente virtualizados. Estos controladores aumentan ampliamente el rendimiento de red y la E/S de dispositivo de bloque para huéspedes completamente virtualizados.
CPU virtualizado	Un sistema tiene una cantidad de CPU virtuales (VCPU) relativas al número de núcleos de procesador físico. El número de VCPU es finito y representa el número total de VCPU que se pueden asignar a máquinas virtuales huéspedes.
Direcciones MAC	La dirección de Control de acceso de medios es la dirección de hardware para el controlador de interfaz de red. En el contexto de virtualización las direcciones se deben generar para interfaces de red virtuales con cada MAC en su dominio local único.
dispositivo phy	The phy device parameter allows guest's to access physical disks. Physical disks includes: • Volúmenes LVM (por ejemplo, **`/dev/VolGroup00/LogVol02`**), • particiones de disco (por ejemplo, **`/dev/sda5`**), y • dispositivos de bloques completos (por ejemplo, **`/dev/sda`**). El modo físico ofrece el mejor desempeño ya que el hipervisor sortea las capas adicionales de software que se encuentren en el equipo, aunque con esto se pierde algo de flexibilidad a la hora de administrar el dispositivo.
E/S	Short for input/output (pronounced "eye-oh"). The term I/O describes any program, operation or device that transfers data to or from a computer and to or from a peripheral device. Every transfer is an output from one device and an input into another. Devices such as keyboards and mouses are input-only devices while devices such as printers are output-only. A writable CD-ROM is both an input and an output device.

Fusión SamePage del Kernel	El módulo de Fusión SamePage del Kernel (KSM, por las iniciales en inglés de Kernel SamePage Merging) es utilizado por el hipervisor KVM de modo de permitir a los huéspedes compartir páginas de memoria idénticas. Las páginas compartidas son por lo general bibliotecas comunes, u otro tipos similares de datos de gran utilización. KSM puede incrementar el desempeño y la densidad ciertos huéspedes, manteniendo estas bibliotecas en caché disponibles para varios de ellos
Hipervisor	The hypervisor is the software layer that abstracts the hardware from the operating system permitting multiple operating systems to run on the same hardware. The hypervisor runs on a host operating system allowing other virtualized operating systems to run on the host's hardware. El hipervisor *Máquinas virtuales basadas en el Kernel* es provisto con Fedora.
Identificador único universal	Un Identificador universal único (UUID) es un método estándar de nomenclatura para dispositivos, sistemas y algunos objetos de software en entornos de informática distribuidos. Los tipos de UUID en virtualización incluyen: identificadores de sistema de archivo `ext2` y `ext3`, identificadores de dispositivos RAID, iSCSI e identificadores de dispositivo LUN, direcciones MAC e identificadores de máquinas virtuales.
Linux con seguridad mejorada	Abreviatura para Security Enhanced Linux o Seguridad mejorada de Linux, SELinux utiliza módulos de seguridad mejorada de Linux (LSM) en el kernel de Linux para proporcionar un rango de políticas de seguridad de mínimo privilegio requerido.
LUN	Un número de unidad lógica (LUN) del inglés Logical Unit Number es un número asignado a una unidad lógica (una entidad de protocolo SCSI).
Maquinas virtual por hardware	Consulte *Virtualización completa*
Máquinas virtuales	Una máquina virtual es una implementación software de una máquina física o un lenguaje de programación (por ejemplo, el entorno en tiempo de ejecución Java o LISP). Las máquinas virtuales en el contexto de virtualización son sistemas operativos en hardware virtualizado.
Máquinas virtuales basadas en el Kernel	KVM (Kernel-based Virtual Machine, Máquina Virtual basada en el Kernel) es una *Virtualización completa* solución para Linux sobre hardware AMD64 e Intel 64. VM es un módulo del Kernel de Linux construido para el Kernel estándar de Linux para empresas de Red Hat. KVM puede ejecutar diferentes sistemas operativos huéspedes, ya sean Windows o Linux, sin tener que modificarlos. KVM es un hipervisor que utiliza las herramientas de virtualización libvirt (virt-manager y virsh).

KVM es un conjunto de módulos de kernel de Linux que administran dispositivos, memoria y APIs de administración para el módulo Hipervisor en sí mismo. Los invitados virtualizados corren como procesos Linux y threads que se controlan con estos módulos.

Migración

Migración es el nombre que recibe el proceso de desplazar un huésped virtualizado de un equipo hacia otro. La migración puede realizarse desconectado (cuando el huésped se interrumpe y luego se traslada), o conectado o en vivo (cuando el huésped es desplazado y trasladado sin interrupción). Los huéspedes KVM totalmente virtualizados pueden ser migrados.

La migración es una función clave de la virtualización ya que el software es totalmente independiente del hardware. La migración es útil para:

- Equilibrio de carga - los huéspedes pueden ser trasladados hacia equipos de menor utilización cuando alguno se encuentre sobrecargado.
- Conmutación por error de hardware - cuando algún dispositivo de hardware del equipo empiece a funcionar erróneamente, los huéspedes pueden ser realojados en forma segura, de modo de permitir que el equipo problemático sea desconectado y reparado.
- Ahorro de energía - los huéspedes pueden ser redistribuidos hacia otros equipos, de modo de permitir desconectar los equipos originarios para ahorrar energía, y abaratar costos en períodos de escasa utilización.
- Migración geográfica - los huéspedes pueden ser trasladados hacia otras ubicaciones para disminuir la latencia, o por circunstancias de fuerza mayor.

Almacenamiento compartido o en redes se utiliza para almacenar imágenes de huésped. Sin migración de almacenamiento compartido esto no es posible.

Un migración offline suspende el huésped, y luego traslada una imagen de su memoria hacia el equipo elegido. El huésped es reiniciado en el equipo de destino y la memoria que el huésped utilizaba en el equipo anterior es liberada.

El tiempo de una migración depende del ancho de banda de la red y de la latencia. Un huésped con 2GB de memoria tarda varios segundos en un enlace Ethernet de 1 Gbit.

Una migración en vivo mantiene al huésped ejecutándose en el equipo de origen y comienza a desplazar la memoria sin interrumpirlo. Todas las páginas de memoria modificadas son rastreadas y enviadas a su destino mientras la imagen es enviada. La memoria se actualiza con las páginas modificadas. El proceso continúa hasta que la cantidad de tiempo de pausa permitida para

	el huésped es idéntica a la cantidad de tiempo estipulada para que las últimas páginas sean transferidas. KVM calcula el tiempo restante e intenta transferir la mayor cantidad de archivos de páginas desde la fuente hacia al destino, hasta KVM considere que la la cantidad de páginas restantes puede ser transferida durante un muy breve espacio de tiempo, mientras el huésped se encuentre en pausa. Los registros son cargados en el nuevo equipo, y el huésped entonces es reanudado en el equipo de destino. Si el huésped no puede ser fusionado (que es lo que sucede cuando las cargas son excesivas), es puesto en pausa y se inicia entonces una migración desconectada. El tiempo que una migración desconectada tarda depende del ancho de banda de red y de la latencia como también de la actividad en el huésped. Si el huésped está utilizando E/S importante o CPU la migración utilizará más tiempo.
Para-virtualización	Para-virtualization uses a special kernel, sometimes referred to as the Xen kernel or the *kernel-xen* package. Para-virtualized guest kernels are run concurrently on the host while using the host's libraries and devices. A para-virtualized installation can have complete access to all devices on the system which can be limited with security settings (SELinux and file controls). Para-virtualization is faster than full virtualization. Para-virtualization can effectively be used for load balancing, provisioning, security and consolidation advantages. A partir de Fedora 9 ya no se necesitará un kernel especial. Una vez se haya aceptado este parche dentro del árbol principal de Linux todos los kernel de Linux después de esta versión tendrán para-virtualización habilitada o disponible.
Para-virtualizado	Consulte *Para-virtualización*,
Paso a través de PCI	El hipervisor KVM ofrece soporte para asociar dispositivos PCI en el sistema del equipo anfitrión para poder virtualizar huéspedes. El paso a través de PCI permite que los huéspedes tengan acceso exclusivo a dispositivos PCI para una gran variedad de tareas. El paso PCI permite que los dispositivos PCI aparezcan y se comporten como si se encontraran físicamente asociados con el sistema operativo huésped.
Sistema huésped	También conocidas como huéspedes, máquinas virtuales, servidores virtuales o dominios.
Virtualización	Virtualización es un término general de informática aplicado a la ejecución de software (generalmente sistemas operativos), al mismo tiempo que se ejecutan otros programas en el sistema, y de manera aislada de ellos. La mayoría de las implementaciones de virtualización actuales, utilizan un hipervisor, esto es, una capa de software colocada sobre un sistema operativo de modo de poder abstraer un determinado hardware. El hipervisor permite que múltiples sistemas operativos sean ejecutados en el mismo sistema físico, al brindarle hardware virtualizado al sistema operativo huésped. Existen varios métodos para virtualizar sistemas operativos:

- Una virtualización asistida por hardware es la técnica utilizada para virtualizaciones completas mediante KVM (definición: *Virtualización completa*)
- La para-virtualización es una técnica utilizada por Xen para ejecutar huéspedes de Linux (definición: *Para-virtualización*)
- Software virtualization or emulation. Software virtualization uses binary translation and other emulation techniques to run unmodified operating systems. Software virtualization is significantly slower than hardware-assisted virtualization or para-virtualization. Software virtualization, in the form of QEMU or BORCH, works in Fedora, it's just slow.

Fedora ofrece soporte para una virtualización completa, asistida por hardware, con el hipervisor KVM.

Virtualización completa

KVM utiliza una virtualization completa y asistida por harware. La virtualización completa utiliza las funciones del hardware del procesador para proporcionar abstracción total del sistema físico subyacente (*Bare-metal*), y crea una nueva máquina virtual en el cual los sistemas operativos huéspedes puedan ejecutarse. No se necesita ninguna modificación en el sistema operativo huésped. El sistema operativo huésped y cualquiera de sus aplicaciones no son conscientes del entorno virtualizado, y se ejecutan normalmente. Una para-virtualization requiere una versión modificada del sistema operativo Linux.

Apéndice B. Historial de revisiones

Revisión 13 **Wed Apr 23 2010** **Christopher Curran** *ccurran@redhat.com*

Actualización y presentación de contenidos en Fedora

Apéndice C. Colofón

Este manual está escrito en el formato de DocBook XML v4.

Este libro se fundamenta en el trabajo de Jan Mark Holzer y Chris Curran.

Otros reconocimientos van para:

- Don Dutile, contribuyó con la edición técnica para la sección de controladores de paravirtualización.
- Barry Donahue, contribuyó con la edición técnica para la sección de controladores de paravirtualización.
- Rick Ring, contribuyó con la edición técnica para la sección sobre el programa de administración de máquinas virtuales.
- Michael Kearey, contribuyó con la edición técnica para las secciones sobre el uso de archivos de configuración en XML con virsh y controladores virtualizados de disquetes.
- Marco Grigull, contribuyó con la edición técnica para las sección de rendimiento y compatibilidad de software.
- Eugene Teo, contribuyó con la edición técnica para la sección de administración de huéspedes con virsh.

Jeffrey Fearn, desarrollador de Publican, la herramienta de publicación que produjo este libro.

Traductores

Debido a limitaciones técnicas, los traductores mencionados en esta sección son aquellos que han trabajado en versiones anteriores de la *Guía de virtualización para Linux de empresas de Red Hat* y de la *Guía de virtualización de Fedora*.

Para saber quiénes han traducido la versión actual de esta guía, por favor visite *https://fedoraproject.org/wiki/Fedora_13_Documentation_Translations_-_Contributors*. Esos traductores serán mencionados en los créditos de las versiones posteriores de esta guía.

- Chino simplificado
  - Leah Wei Liu
- Chino tradicional
  - Chester Cheng
  - Terry Chuang
- Japonés
  - Kiyoto Hashida
- Coreano
  - Eun-ju Kim
- Holandés

    - Geert Warrink
- Francés
    - Sam Friedmann
- Alemán
    - Hedda Peters
- Griego
    - Nikos Charonitakis
- Italiano
    - Silvio Pierro
    - Francesco Valente
- Portugués (Brasil)
    - Glaucia de Freitas
    - Leticia de Lima
- Español
    - Domingo Becker
    - Héctor Daniel Cabrera
    - Angela Garcia
    - Gladys Guerrero
- Ruso
    - Yuliya Poyarkova